

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT
QUESTIONS

Information Systems Concepts

1. (a) What is information? Discuss its attributes.
(b) 'In modern business perspective, information systems have far reaching effects for smooth and efficient operations'. Discuss some of these important implications of information systems in business.
2. (a) Describe the features of Transaction Processing Systems in brief.
(b) Discuss major constraints, which come in the way of operating an information system.

Software Development Life Cycle Methodology

3. (a) Explain the strengths and weaknesses of Prototyping model.
(b) 'Requirements Analysis phase includes a thorough and detailed understanding of the current system, identifications of the areas that need modifications to solve the problem, the determination of user/managerial requirements and to have fair idea about various systems development tools'. Briefly discuss the activities, which are performed in this phase.
4. (a) Describe physical design principles in brief.
(b) 'Management should establish acquisition standards that address the same security and reliability issues as development standards.' What are the areas that should be focused by acquisition standards?
5. (a) Explain various categories of system maintenance.
(b) 'Large organizations would naturally tend to adopt a sophisticated and objective approach to validate the vendor's proposal'. What are the validation methods that may be used for this purpose?

Control Objectives

6. (a) Discuss the functions of an IS Auditor in brief.
(b) 'The objective of controls is to reduce or if possible, eliminate the causes of the exposure to potential loss. Exposures are potential losses due to threats materializing. All exposures have causes'. Discuss some categories of exposures in brief and also discuss some critical control considerations in a computerized environment.
7. (a) 'Audit trails can be used to support security objectives in three basic ways'. Briefly discuss these ways.
(b) Discuss auditors' role in authorization controls.

FINAL EXAMINATION :MAY, 2011

8. (a) What are the activities that should be reviewed by the team during a Post Implementation Review, according to their terms of reference?
- (b) What are the weaknesses associated with packet filtering firewalls?

Testing – General and Automated Controls

9. (a) Describe the information developed in the testing phase that the auditor should document.
- (b) What are the activities that should be determined by a reviewer, while reviewing the hardware plan?

Risk Assessment Methodologies and Applications

10. (a) 'Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied'. What are the main reasons of this gap?
- (b) In addition to the 'establishing casual relationship', what are the other risk mitigation measures?

Business Continuity Planning and Disaster Recovery Planning

11. (a) What should be the goals of a business continuity plan? Explain in brief.
- (b) Explain various tasks to be undertaken in 'Business Impact Analysis' phase.

An Overview of Enterprise Resource Planning (ERP)

12. (a) What are the main benefits achieved by implementing the ERP package?
- (b) 'ERP implementation also engenders a host of fears.' What are those fears? Explain in brief.

Information Systems Auditing Standards, Guidelines, Best Practices

13. (a) 'The documentation of ISO 27001 consists of evidence of action undertaken under establishment of various activities'. Explain these activities in brief.
- (b) Discuss controls and objectives of security policy.
14. (a) Discuss various domains under COBIT in brief.
- (b) 'The Business Perspective is the name given to the collection of best practices that is suggested to address some of the issues often encountered in understanding and improving IT service provision, as a part of the entire business requirements for high IS quality management'. What are these issues?

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

15. (a) State the major points required to be stated by a good security policy.
- (b) Discuss the points that need to be taken into account for the proper implementation of Physical and Environmental Security.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Information Technology (Amendment) Act 2008

16. (a) Define the following terms with respect to Information Technology (Amendment) Act, 2008:
- (i) Access
 - (ii) Appropriate Government
 - (iii) Computer Network
 - (iv) Secure System
- (b) Discuss the use of electronic records and electronic signature in Government and its agencies with respect to the Section 6 of Information Technology (Amendment) Act, 2008.
17. (a) Describe Secure Electronic Signature with respect to the Section 15 of Information Technology (Amendment) Act, 2008.
- (b) Discuss the duties of Certifying Authorities with respect to the Section 30 of Information Technology (Amendment) Act, 2008.

Questions based on Short Notes

18. Write short notes on the following:
- (a) Text Processing Systems
 - (b) Electronic Document Management Systems
 - (c) Deterministic and Probabilistic Systems
19. Write short notes on the following:
- (a) Strengths of Incremental Model
 - (b) Program Debugging
 - (c) System Testing
20. Write short notes on the following:
- (a) Detective Controls
 - (b) Corrective Controls
 - (c) Application level Firewalls

Questions based on Case Studies

21. ABC Technologies Ltd. is in the development of web applications for various domains. For the development purposes, the company is committed to follow the best practices suggested by SDLC. A system development methodology is a formalized, standardized, and documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an

FINAL EXAMINATION :MAY, 2011

information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations.

Read the above carefully and answer the following:

- (a) Describe accountants' involvement in development work in brief.
 - (b) 'Waterfall approach is one of the popular approaches for system development'. Explain the basic principles of this approach.
 - (c) Briefly describe major characteristics of Agile Methodology.
22. XYZ Associates is dealing in the information systems audit and particularly deals with the auditing of controls. Controls are defined as "the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected". The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing an effective information control framework, which comprise policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved.

Read the above carefully and answer the following:

- (a) Explain the aspects to consider while reviewing the organizational and management controls in an information system.
 - (b) Discuss data processing controls in brief.
 - (c) Briefly discuss auditors' role in application software acquisition/selection process.
 - (d) What are the costs involved in the implementation and operation of the controls?
23. PQR Enterprises is engaged in a business of manufacturing electronic products. The company is in the process of automation of its various business processes. During this automation, technical consultant of the company suggested to perform the risk assessment activity and to mitigate the assessed risks. Basically, risk assessment seeks to identify 'which business processes and related resources are critical to the business', 'what threats or exposures exist, that can cause an unplanned interruption of business processes', and 'what costs accrue due to an interruption'. There are various analytical procedures that are used to determine various risks, threats, and exposures, faced by an organization. These are known as Business Impact Analysis (BIA), Risk Impact Analysis (RIA) and so on.

Read the above carefully and answer the following:

- (a) Define Systematic Risks and Unsystematic Risks with the help of examples.
- (b) There are various techniques that are available to assess and evaluate risks, namely, Judgement and Intuition, Delphi Approach, Scoring, Qualitative Techniques, and Quantitative Techniques. Explain Delphi and Scoring approaches in brief.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (c) In automation of the business modules, retention of electronic records is an important activity. How Information Technology (Amendment) Act 2008 addresses this issue with reference to its Section 7?
24. ABC Group of Industries is in the process of launching a new business unit viz. ABC Consultants Ltd. to provide various consultancy services to the organizations worldwide, to assist them in the computerization of their business modules. It involves a number of activities starting from the capturing of the requirements to the maintenance. Business continuity and disaster recovery planning are two key activities in this entire process, which must be taken care *right from the beginning*. Business continuity focuses on maintaining the operations of an 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 maintain operations and there is a service disruption. This plan focuses on restarting the operations using a prioritized resumption list.

Read the above carefully and answer the following:

- (a) What are the issues that are emphasized by the methodology for developing a business continuity plan?
- (b) Explain the objectives of performing Business Continuity Planning tests.
- (c) What are the issues, written in a contract that should be ensured by security administrators if a third-party site is to be used for backup and recovery purposes?
25. XYZ Ltd. is a leading company in FMCG sector and has a large number of coffee chains across India. It uses ERP system for all its business operations and for recording sales at each outlet. It has customized ERP, which is connected to a central server. 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) An ERP system is not only the integration of various organization processes. Any system has to possess few key characteristics to qualify for a true ERP solution. What are these features?
- (b) 'Access Controls plays a key role in the implementation of information security policies'. Explain its detailed control and objectives.
- (c) Describe 'Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security' with respect to the Section 69B of Information Technology (Amendment) Act, 2008.
- (d) Briefly explain the tasks that are to be performed during the post-implementation period of an ERP package.

SUGGESTED ANSWERS / HINTS

1. (a) **Information:** Information is data that have been put into a meaningful and useful context. It has been defined by Davis and Olson as - "Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision". For example, data regarding sales by various salesmen can be merged to provide information regarding total sales through sales personnel. This information is of vital importance to a marketing manager who is trying to plan for future sales.

The term 'data' and 'information' are often used interchangeably. However, the relation of data to information is that of raw material to finished product. A data processing system processes data to generate information on which business decisions are based. Therefore, the quality of information determines the quality of action or decision. The management plays the part of converting the information into action through the familiar process of decision-making. Therefore, Information plays a vital role in the survival of a business.

Attributes of Information

Some of the important attributes of useful and effective information are as follows:

- (i) **Availability:** Availability or Timeliness is a very important property of information. If information is not available at the time of need, it is useless. Data is organized in the form of facts and figures in databases and files from where various information is derived for useful purpose.
- (ii) **Purpose:** Information must have purposes at the time it is transmitted to a person or machine, otherwise it is simple data. Information communicated to people has a variety of purposes because of the variety of activities performed by them in business organizations. The basic purpose of information is to inform, evaluate, persuade, and organize.

It helps in creating new concepts, identifying problems, solving problems, decision making, planning, initiating, and controlling. These are just some of the purposes to which information is directed to human activity in business organizations.

- (iii) **Mode and format:** The modes of communicating information to humans are sensory (through sight, hear, taste, touch and smell) but in business they are 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. Therefore, all the statistical rules of compiling statistical tables and presenting information by means of diagram, graphs, curves, etc., should be considered. Format of information dissemination is a matter of imagination and perception. It should

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

be simple, relevant and should highlight important points but should not be too cluttered up.

- (iv) **Decay:** Value of information usually decays with time and usage and so it should be refreshed from time to time. For example, we access the running score sheet of a cricket match through Internet sites and this score sheet is continually refreshed at a fixed interval or based on status of the match. Similarly, in highly fluctuating share market, a broker is always interested about the latest information of a particular stock/s.
- (v) **Rate:** The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive. Quantitatively, the rate for humans may be measured by the number of numeric characters transmitted per minute, such as sales reports from a district office. For machines, the rate may be based on the number of bits of information per character (sign) per unit of time.
- (vi) **Frequency:** The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little changes that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.
- (vii) **Completeness:** The information should be as complete as possible. For example - Hartz's model for investment decisions provides information on mean, standard deviation and the shape of the distribution of ROI and NPV. With this complete information, the manager is in a much better position to decide whether or not to undertake the venture.
- (viii) **Reliability:** It is just not authenticity or correctness of information; rather technically it is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say that the information is reliable.
- (ix) **Validity:** It measures the closeness of the information to the purpose, which it purports to serve. For example, some productivity measure may not measure, for the given situation, what they are supposed to do e.g., the real rise or fall in productivity. The measure suiting the organization may have to be carefully selected or evolved.
- (x) **Quality:** Quality refers to the correctness of information. Information is likely to be spoiled by personal bias. For example, an over-optimistic salesman may give rather too high estimates of the sales. This problem, however, can be circumvented by maintaining records of salesman's estimates and actual sales and deflating or inflating the estimates in the light of this.
- (xi) **Transparency:** If information does not reveal directly what we want to know for decision-making, it is not transparent. For example, total amount of

FINAL EXAMINATION :MAY, 2011

advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.

(xii) **Value of information:** It is defined as a difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

(xiii) **Adequacy:** To be useful, information must be adequate so that the desired actions can be initiated. Required information should flow in different directions within the organization. Further, the type of information that flows within the organization or across it, should have adequate and relevant contents.

(b) Some of important implications of information systems in business are as follows:

- Information system helps managers in effective decision-making to achieve the organizational goal.
- Based on well-designed Information system, an organization will gain edge in the competitive environment.
- Information systems help in taking right decision at the right time.
- Innovative ideas for solving critical problems may come out from good Information system.
- Knowledge gathered through Information system may be utilized by managers in unusual situations.
- Information system is viewed as a process; it can be integrated to formulate a strategy of action or operation.

2. (a) **Features of a Transaction Processing System (TPS)**

Some of the important features of TPS are given as follows:

- **Large volume of data:** As TPS is transaction-oriented, it generally consists of a large volume of data and thus requires greater storage capacity. Its major concern is to ensure that the data regarding the economic events in the organizations are captured quickly and correctly.
- **Automation of basic operations:** Any TPS aims at automating the basic operations of a business enterprise and plays a critical role in the day-to-day functioning of the enterprise. Any failure in the TPS for a short period of time can play havoc with the functioning of the enterprise. Thus, TPS is an important source of up-to-date information regarding the operations in the enterprise.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- **Benefits are easily measurable:** TPS reduces the workload of the people associated with the operations and improves their efficiency by automating some of the operations. Most of these benefits of the TPS are tangible and easily measurable. Therefore, cost benefit analysis regarding the desirability of TPS is easy to conduct. As the benefits from TPS are mainly tangible, the user acceptance is easy to obtain.
 - **Source of input for other systems:** TPS is the basic source of internal information for other information systems. Heavy reliance by other information systems on TPS for this purpose makes TPS important for tactical and strategic decisions as well.
- (b) Major constraints, which come in the way of operating an information system are given as follows:
- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing and operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
 - Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts, depends upon the need and importance of a function for which MIS can be installed first.
 - Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.
 - Non-availability of cooperation from staff is a crucial problem which should be handled tactfully. This task should be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.
3. (a) **Strengths:** Some of the major strengths of Prototyping model are given as follows:
- Improves both user participation in system development and communication among project stakeholders.
 - Especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.
 - Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
 - Helps to easily identify confusing or difficult functions and missing functionality.
 - May generate specifications for a production application.
 - Encourages innovation and flexible designs.

FINAL EXAMINATION :MAY, 2011

- Provides quick implementation of an incomplete, but functional application.
- Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of these users' needs and requirements than does the traditional system development approach.
- A very short time period (e.g., a week) is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
- Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

Weaknesses: Some of the major weaknesses of Prototyping model are given as follows:

- Approval process and control are not strict.
- Incomplete or inadequate problem analysis may occur whereby only the most obvious and superficial needs will be addressed, resulting in current inefficient practices being easily built into the new system.
- Requirements may frequently change significantly.
- Identification of non-functional elements is difficult to document.
- Designers may prototype too quickly, without sufficient upfront user needs analysis, resulting in an inflexible design with narrow focus that limits future system potential.
- Prototype may not have sufficient checks and balances incorporated.
- Prototyping can only be successful if the system users are willing to devote significant time in experimenting with the prototype and provide the system developers with change suggestions. The users may not be able or willing to spend the amount of time required under the prototyping approach.
- The interactive process of prototyping causes the prototype to be experimented with quite extensively. Because of this, the system developers are frequently tempted to minimize the testing and documentation process of the ultimately approved information system. Inadequate testing can make the approved system error-prone, and inadequate documentation makes this system difficult to maintain.
- Prototyping may cause behavioral problems with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands for improvements as well as dissatisfaction and

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

impatience by users when they have to go through too many interactions of the prototype.

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

(b) The following major activities are performed in this phase:

- To identify and consult the stake owners to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine priorities;
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like- interviewing, research/document collection, questionnaires, observation;
- To model activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

4. (a) **Physical Design Principles:** Major physical design principles are described as follows:

- There is a tendency to develop merely one design and consider it the final product. However the recommended procedure is to design two or three alternatives and choose the best one on pre-specified criteria.
- The design should be based on the analysis.
- The software functions designed should be directly relevant to business activities.
- The design should follow standards laid down. For instance, the user interface should have consistent color scheme, menu structure, location of error message and the like.
- The design should be modular.

(b) Acquisition standards should focus on the following issues:

- Ensuring security, reliability, and functionality already built into a product.
- Ensuring managers complete appropriate vendor contract, and licensing reviews and acquiring products compatible with existing systems.

FINAL EXAMINATION :MAY, 2011

- Including invitations-to-tender and request-for-proposals. Invitations-to-tender involve soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software. Request-for-proposals involve soliciting bids when acquiring off-the-shelf or third-party developed software.
- Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.

5. (a) System Maintenance can be categorized in the following parts :

- **Scheduled maintenance:** This is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.
- **Rescue maintenance:** It refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- **Corrective maintenance:** It deals with fixing bugs in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors.

The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.

- **Adaptive maintenance:** It consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.
- **Perfective maintenance:** This mainly deals with accommodating to new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- **Preventive maintenance:** It concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

(b) Some of the validation methods used for vendors' proposals are given as follows:

- (i) **Checklists:** It is the most simple and rather a subjective method for validation and evaluation. The various criteria are put in check list in the form of suitable questions against which the responses of various vendors are validated.

For example: Support Service Checklists may have parameters like– Performance; System development; Maintenance; Conversion; Training; Back-up; Proximity; Hardware; Software.

- (ii) **Point-Scoring Analysis:** Point-scoring analysis provides an objective means of selecting a final system. There are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. Thus, even for a small business, the evaluators must consider such issues as the company's data processing needs, its in-house computer skills, vendor reputations, software costs, and so forth.

Following Table illustrates a Point Scoring Analysis list:

Software Evaluation Criteria	Possible points	Vendor A	Vendor B	Vendor C
Does the software meet all mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8
Is the performance (speed, accuracy, reliability, etc.) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and test-driven?	9	8	8	7
Does the software have an adequate warranty?	8	6	7	6
Is the software flexible and easily maintained?	8	5	7	5
Is online inquiry of files and records possible?	10	8	9	7
Will the vendor keep the software up to date?	10	8	8	7
Totals	123	94	106	85

FINAL EXAMINATION :MAY, 2011

- (iii) **Public Evaluation Reports:** Several consultancy agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard. This method has been frequently and usefully employed by several buyers in the past. For those criteria, however, where published reports are not available, resort would have to be made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of facts.
 - (iv) **Bench marking problem for vendor's proposals :** Benchmarking problems for vendors' proposals are sample programs that represent at least a part of the buyer's primary computer work load and include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs. That is, benchmarking problems are oriented towards testing whether a computer offered by the vendor meets the requirements of the job on hand of the buyer.
 - (v) **Test problems:** Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to translate the source code (program in an assembly or a high level language) into the object code (machine language), response time for two or more jobs in multi-programming environment, overhead requirements of the operating system in executing a user program, length of time required to execute an instruction, etc. The results achieved by the machine can be compared and price performance judgement can be made. It must be borne in mind, however, that various capabilities to be tested would have to be assigned relative weight-age.
6. (a) Mainly, IS auditors review risks relating to IT systems and processes; however, some of the major functions are mentioned as under:
- Inadequate information security (e.g. missing or out of date antivirus controls, open computer ports, open systems without password or weak passwords etc.)
 - Inefficient use of corporate resources, or poor governance (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.)
 - Ineffective IT strategies, policies and practices (including lack of policies for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.)
 - IT-related frauds (including phishing, hacking etc.)
- (b) Some categories of exposures are:
- Errors or omissions in data, procedure, processing, judgment and comparison.
 - Improper authorizations and improper accountability with regards to procedures, processing, judgment and comparison.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- Inefficient activity in procedures, processing and comparison.

Some of the critical control considerations in a computerized environment are given as follows:

- Lack of management understanding of IS risks and lack of necessary IS and related controls.
- Absence or inadequate IS control framework.
- Absence of or weak general controls and IS controls.
- Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff.
- Complexity of implementation of controls in distributed computing environments and extended enterprises.
- Lack of control features or their implementation in highly technology driven environments.
- Inappropriate technology implementations or inadequate security functionality in technologies implemented.

7. (a) Audit trails can be used to support security objectives in following three ways :

- (i) *Detecting Unauthorized Access:* Detecting unauthorized access can occur in 'real time' or 'after-the-fact'. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. 'After-the-fact' detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
- (ii) *Reconstructing Events:* Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that exist at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- (iii) *Personal Accountability:* Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individual are likely to violate an organization's security policy if they know that their actions are recorded in an audit log.

FINAL EXAMINATION :MAY, 2011

- (b) Authorization controls ensure that all the information and data entered or used in processing is authorized by management, and responsible representatives of events that actually occurred. Auditors' role in authorization controls involves the following activities:
- Transactions in an application system are manually authorized, the controls that ensure that no unauthorized modifications take place after authorization and prior to establishing input controls. Determine if the proper level of management is authorizing the transaction activity.
 - If transaction authorization is facilitated by logical access restrictions, select a sample of access rules applying to transaction input and update, and verify if the appropriate people have these capabilities.
 - Identify any allowable overrides or bypasses of data validation and edit checks e.g. authorization, monitoring, etc. Determine who can do the overrides and verify that they are in a management position that should have this authority. Are all uses of the override features automatically logged so these actions can be subsequently analyzed for appropriateness?
 - Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is as audit trail for all urgent matters.
 - Review by IT management to monitor, and approve all changes to hardware, software, and personnel responsibilities.
 - Assigned and authorized responsibilities to those involved in the change and monitor their work with adequate segregation of duties.
8. (a) During a Post Implementation Review, the team should review the following activities, according to their terms of reference:
- the main functionality of the operational system against the User Requirements Specification;
 - system performance and operation;
 - the development techniques and methodologies employed;
 - estimated time-scales and budgets, and identify reasons for variations;
 - changes to requirements, and confirm that they were considered authorized and implemented in accordance with change and configuration management standards;
 - set out findings, conclusions and recommendations in a report for the authorising authority to consider;
 - In addition to reviewing of the functionality delivered by the new system, the review team will also need to look back to the Business Case on which the

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

system was originally based to confirm that all the anticipated benefits, both tangible and intangible, have been delivered. This will involve investigating the reasons behind benefits that were not achieved, perhaps involving recommendations for remedial action, and using survey techniques to establish the extent to which intangible benefits (such as improved staff morale) have been realised.

- (b) Weaknesses associated with packet filtering firewalls include the following:
- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.
 - Logging functionality is limited to the same information used to make access control decisions.
 - Most of such firewalls do not support advanced user authentication schemes.
 - Firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
 - The firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.
9. (a) Information developed in the testing phase that the auditor should document includes the following:
- An understanding of the information systems that are relevant to the audit objectives;
 - IS Control objectives and activities relevant to the audit objectives;
 - By level (e.g., entitywide, system, business process application) and system sublevel (e.g., network, operating system, infrastructure applications), a description of control techniques used by the entity to achieve the relevant IS control objectives and activities;
 - By level and sublevel, specific tests performed, including related documentation that describes the nature, timing, and extent of the tests;
 - evidence of the effective operation of the control techniques or lack thereof (e.g. memos describing procedures and results, output of tools and related analysis);
 - if a control is not achieved, any compensating controls or other factors and the basis for determining whether they are effective;
 - the auditor's conclusions about the effectiveness of the entity's IS controls in achieving the control objective; and
 - for each weakness, whether the weakness is a material weakness, significant deficiency or just a deficiency, as well as the criteria, condition, cause, and effect if necessary to achieve the audit objectives.

FINAL EXAMINATION :MAY, 2011

- (b) Reviewers should review the hardware acquisition plan to determine:
- Whether the IS management has issued written policy statements regarding the acquisition of hardware.
 - Whether the criteria for the acquisition of hardware are laid out and procedures and forms established to facilitate the acquisition approval process.
 - Whether the hardware acquisition plan is in concurrence with the strategic business plan of management.
 - Whether there is awareness of the budget constraints.
 - Whether the requests for the acquisition of hardware are supported by cost benefit analysis.
 - Whether all hardware are purchased through the IS purchasing department to take advantage of volume discounts or other quality benefits.
 - Whether the environment is conducive and space is adequate to accommodate the current and new hardware.
 - Whether IS management's hardware acquisition plan has taken into consideration technological obsolescence of the installed equipped, as well the new equipment in the acquisition plan.
 - Whether there has been a consideration of lease expirations on current equipment.
 - Whether documentation for hardware and software specifications, installation requirements, warranties, guarantees and likely lead-time associated with planned acquisitions is properly maintained.

10. (a) Some of the main reasons of this gap are given as follows:
- Widespread use of technology;
 - Interconnectivity of systems;
 - Elimination of distance, time and space as constraints;
 - Unevenness of technological changes;
 - Devolution of management and control;
 - Attractiveness of conducting unconventional electronic attacks against organisations; and
 - External factors such as legislative, legal and regulatory requirements or technological developments.
- (b) In addition to 'establishing causal relationship', other risk mitigation measures are:
- Self assessment,
 - Calculating reserves and capital requirements,

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- Creating culture supportive of risk mitigation,
 - Strengthening internal controls, including internal and external audit of systems, processes and controls, including IS audit and assurance),
 - Setting up operational risks limits (so business will have to reduce one or more of frequency of loss, severity of loss or size of operations),
 - Setting up independent operational risk management departments,
 - Establishing a disaster recovery plan and backup systems,
 - Insurance, and
 - Outsourcing operations with strict service level agreements so operational risk is transferred.
11. (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;
 - facilitate effective co-ordination of recovery tasks; and
 - reduce the complexity of the recovery effort.
- (b) Various tasks, which are to be undertaken in 'Business Impact Analysis' 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 organisation in the event of a disaster, e.g. financial reputation, etc.
12. (a) Main benefits achieved by implementing the ERP packages are given as follows:
- Gives Accounts personnel, increased control of invoicing & payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations.

FINAL EXAMINATION :MAY, 2011

- Reduces paper documents by providing on-line formats for quickly entering and retrieving information.
- Improves timeliness of information by permitting posting daily instead of monthly.
- Greater accuracy of information with detailed content, better presentation, satisfactory for the auditors.
- Improved cost control.
- Faster response and follow-up on customers.
- More efficient cash collection.
- Better monitoring and quicker resolution of queries.
- Enables quick response to change the business operations and market conditions.
- Helps to achieve competitive advantage by improving its business processes.
- Improves supply-demand linkage with remote locations and branches in different countries.
- Provides a unified customer database usable by all applications.
- Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
- Improves information access and management throughout the enterprise.
- Provides solution for problems like Y2K and Single Monetary Unit (SMU) or Euro Currency.

(b) Some of these fears are given as under:

- Job redundancy.
- Loss of importance as information is no longer an individual prerogative.
- Change in job profile.
- An organizational fear of loss of proper control and authorization.
- Increased stress caused by greater transparency.
- Individual fear of loss of authority.

Balancing the expectations and fears is a very necessary part of the implementation process.

13. (a) The documentation of ISO 27001 consists of evidence of action undertaken under establishment of the following:

- Management control;

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability;
 - Procedure adopted to implement control under Implementation clause;
 - ISMS management procedure;
 - Document Control: The issues focused under this clause would be:
 - Ready availability,
 - Periodic review,
 - Maintain version control,
 - Withdrawal when obsolete, and
 - Preservation for legal purpose.
 - Records : The issues involved in record maintenance are as follows:
 - Maintain to evidence compliance to Part 2 of BS7799,
 - Procedure for identifying, maintaining, retaining, and disposing of such evidence,
 - Records to be legible, identifiable and traceable to activity involved, and
 - Storage to augment retrieval, and protection against damage.
- (b) The detailed controls and objectives of security policy 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.
14. (a) COBIT covers four domains which are given as follows:
- Plan and Organize,
 - Acquire and Implement,
 - Deliver and Support, and
 - Monitor and Evaluate.

FINAL EXAMINATION :MAY, 2011

Plan and Organize

The Plan and Organize domain covers the use of information & technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT. The following table lists the IT processes contained in the Planning and Organization domain.

IT PROCESSES Plan and Organize

PO1	Define a Strategic IT Plan and direction
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects

Acquire and Implement

The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components. The following table lists the IT processes contained in the Acquire and Implement domain.

IT PROCESSES Acquire and Implement

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredited Solutions and Changes

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Deliver and Support

The Deliver and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training. The following table lists the IT processes contained in the Deliver and Support domain.

IT PROCESSES Deliver and Support

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

Monitor and Evaluate

The Monitor and Evaluate domain deals with a company's strategy in assessing the needs of the company and whether or not the current system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors. The following table lists the IT processes contained in the Monitor and Evaluate domain.

IT PROCESSES Monitor and Evaluate

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

FINAL EXAMINATION :MAY, 2011

(b) These issues are given as follows:

- Business Continuity Management describes the responsibilities and opportunities available to the business manager to improve. In most of the organizations, this is one of the key contributing services to business efficiency and effectiveness.
- Surviving Change: IT infrastructure changes can impact the manner in which business is conducted or the continuity of business operations. It is important that business managers take notice of these changes and ensure that steps are taken to safeguard the business from adverse side effects.
- Transformation of business practice through radical change, helps to control IT and to integrate it with the business.
- Partnerships and outsourcing.

15. (a) A good security policy should clearly state the following :

- Purpose and Scope of the Document and the intended audience,
- The Security Infrastructure,
- Security policy document maintenance and compliance requirements,
- Incident response mechanism and incident reporting,
- Security organization Structure,
- Inventory and Classification of assets,
- Description of technologies and computing structure,
- Physical and Environmental Security,
- Identity Management and access control,
- IT Operations management,
- IT Communications,
- System Development and Maintenance Controls,
- Business Continuity Planning,
- Legal Compliances,
- Monitoring and Auditing Requirements, and
- Underlying Technical Policy.

(b) For the proper implementation of Physical and Environment Security, the following points are needed to be taken into account:

- Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
- The IT infrastructure must be physically protected.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- Access to secure areas must remain limited to authorized staff only.
 - Confidential and sensitive information and valuable assets must always be securely locked away when not in use.
 - Computers never be left unattended whilst displaying confidential or sensitive information or whilst logged on to systems.
 - Equipments must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities.
 - Equipment, information or software must not be taken off-site without proper authorization.
 - Wherever practical, premises housing computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.
 - The location of the equipment room(s) must not be obvious. It should be protected against threats of unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.
- 16. (a) (i)** "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
- (ii)** "Appropriate Government" means as respects any matter.
- (a) enumerated in List II of the Seventh Schedule to the Constitution;
 - (b) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;
- (iii)** "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-
- (a) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
 - (b) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;
- (iv)** "Secure System" means computer hardware, software, and procedure that -:
- (a) are reasonably secure from unauthorized access and misuse;
 - (b) provide a reasonable level of reliability and correct operation;
 - (c) are reasonably suited to performing the intended functions; and
 - (d) adhere to generally accepted security procedures;

FINAL EXAMINATION :MAY, 2011

(b) [Section 6] Use of Electronic Records and Electronic Signature in Government and its agencies:

- (1) Where any law provides for
 - (a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
 - (b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
 - (c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.
- (2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe
 - (a) the manner and format in which such electronic records shall be filed, created or issued;
 - (b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

17. (a) [Section 15] Secure Electronic Signature (Substituted vide ITAA 2008) :

An electronic signature shall be deemed to be a secure electronic signature if-

- (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
- (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed

Explanation- In case of digital signature, the "signature creation data" means the private key of the subscriber.

(b) [Section 30] Duties of Certifying Authorities:

This section provides that every Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below: Every Certifying Authority shall-

- (a) make use of hardware, software, and procedures that are secure from intrusion and misuse;
- (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- (c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (**Amended vide ITAA 2008**)

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)
- (cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)
- (d) observe such other standards as may be specified by regulations.

18. (a) Text Processing Systems:

Text processing systems are the most commonly used components of the Office Automation System (OAS). This is so because a large proportion of the office communication takes place in writing by using words of a natural language. Text processing systems automate the process of development of documents such as letters, reports, memos etc. They permit use of standard stored information to produce personalized documents. Such automation reduces keying effort and minimizes the chances of errors in the document.

The text processor may be simple word processing systems or desktop publishing systems. The desktop publishing systems help in quick production of multiple copies of the document with quality printing. The desktop publishing systems are often supported with laser printers, inkjet printers, scanners and other such devices for producing good quality documents.

(b) Electronic Document Management Systems

The computer based document management systems are at capturing the information contained in documents, stored for future reference and communicate the relevant parts to the users as and when required. These systems are linked to the office automation systems such as text processors, electronic message communication systems etc. These systems are very useful in remote access of documents that is almost impossible with manual document management systems. For example, a customer may have a complaint concerning delivery of goods not being in accordance with the delivery instructions in the order. The computer based document management system would enable executives to access the document through his/her notebook computer connected to any telephone line and show it to the customer, his/her order document in the office.

In the case of internal communication, document management systems can prove to be very useful. For example, the loan application form filed in a branch of a bank can be accessed by the sanctioning officer for scrutiny at the head office or any office for scrutiny of loan proposals. With computer based document management systems, location of the executive becomes irrelevant for access to documents. Thus, these systems can be very useful in an office environment where traveling executives share work space in the office.

- (c) **Deterministic System:** A deterministic system operates in a predictable manner wherein the interaction among the parts is known with certainty. If one has a

FINAL EXAMINATION :MAY, 2011

description of the state of the system at a given point in time along with a description of its operation, the next state of the system may be given exactly, without error. An example is a correct computer program, which performs exactly according to a set of instructions.

Probabilistic System: The probabilistic system can be described in terms of probable behavior, but a certain degree of error is always attached to the prediction of 'what the system will do'. An inventory system is an example of a probabilistic system. The average demand, average time for replenishment, etc, may be defined, but the exact value at any given time is not known. Another example is a set of instructions given to a human who, for a variety of reasons, may not follow the instructions exactly as given.

19. (a) **Strengths of Incremental Model**

- (i) Potential exists for exploiting knowledge gained in an early increment as later increments are developed.
- (ii) Moderate control is maintained over the life of the project through the use of written documentation and the formal review and approval/signoff by the user and information technology management at designated major milestones.
- (iii) Stakeholders can be given concrete evidence of project status throughout the life cycle.
- (iv) More flexible – less costly to change scope and requirements.
- (v) Helps to mitigate integration and architectural risks earlier in the project.
- (vi) Allows delivery of a series of implementations that are gradually more complete and can go into production more quickly as incremental releases.
- (vii) Gradual implementation provides the ability to monitor the effect of incremental changes, isolated issues and make adjustments before the organization is negatively impacted.

(b) **Program Debugging**

Debugging is the most primitive form of testing activity, which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compiling means that the program can be successfully converted from the source code written by the programmer into machine language instructions. Debugging can be a tedious task consisting of following four steps:

- Inputting the source program to the compiler,
- Letting the compiler find errors in the program,
- Correcting lines of code that are erroneous, and
- Resubmitting the corrected source program as input to the compiler.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

(c) System Testing

System testing is a process in which software and other system elements are tested as a whole. System testing begins either when the software as a whole is operational or when the well defined subsets of the software's functionality have been implemented. The purpose of system testing is to ensure that the new or modified system functions properly. These test procedures are often performed in a non- production test environment. The types of testing that might be carried out are as follows:

- **Recovery Testing:** This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is properly performed.
- **Security Testing:** This is the process to determine that an Information System protects data and maintains functionality as intended or not. The six basic security concepts that need to be covered by security testing are – confidentiality, integrity, authentication, authorization, availability and non-repudiation. This testing technique also ensures the existence and proper execution of access controls in the new system.
- **Stress or Volume Testing:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.
- **Performance Testing:** In the computer industry, software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

20. (a) **Detective Controls** : These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. The main characteristics of such controls are as follows:

- Clear understanding of lawful activities so that anything, which deviates from these is reported as unlawful, malicious, etc.
- An established mechanism to refer the reported unlawful activities to the appropriate person or group;
- Interaction with the preventive control to prevent such acts from occurring; and
- Surprise checks by supervisor.

FINAL EXAMINATION :MAY, 2011

Examples of detective controls include:

- Hash totals,
- Check points in production jobs,
- Echo control in telecommunications,
- Error message over tape labels,
- Duplicate checking of calculations,
- Periodic performance reporting with variances,
- Past-due accounts report,
- The internal audit functions,
- Intrusion detection system,
- Cash counts and bank reconciliation, and
- Monitoring expenditures against budgeted amount.

(b) **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error, once, it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A business continuity plan is considered to be a significant corrective control. The main characteristics of the corrective controls are:

- Minimize the impact of the threat;
- Identify the cause of the problem;
- Remedy problems discovered by detective controls;
- Get feedback from preventive and detective controls;
- Correct error arising from a problem; and
- Modify the processing systems to minimize future occurrences of the problem.
- Examples of Corrective Controls are:
- Contingency planning,
- Backup procedure,
- Rerun procedures,
- Treatment procedures for a disease,
- Change input value to an application system, and
- Investigate budget variance and report violations.

(c) **Application level Firewalls:** Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.

The primary disadvantages of application-level firewalls are as follows:

The time required to read and interpret each packet slows network traffic. Traffic of certain types may have to be split off before the application-level firewall and passed through different access controls.

Any particular firewall may provide only limited support for new network applications and protocols. They also simply may allow traffic from those applications and protocols to go through the firewall.

21. (a) Accountants' involvement in Development work

Many accountants are uniquely qualified to participate in systems development process because they may be among the few people in an organization, who can combine the knowledge of IT, business, accounting, and internal controls, as well as behavior and communications, to ensure that new systems meet the needs of the user and possess adequate internal controls. They have specialized skills - such as accounting and auditing - that can be applied to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits.

(b) Basic Principles of Waterfall Approach: These principles are given as under:

- Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

(c) Some of the major characteristics of Agile Methodology are as follows:

- Iterative with short cycles enabling fast verifications and corrections;
- Time bound iterative cycles;
- Modularity at development process level;
- People oriented;

FINAL EXAMINATION :MAY, 2011

- Collaborative and communicative working style; and
 - Incremental and convergent approach that minimizes risks and facilitates functional additions.
22. (a) The controls to consider while reviewing the organizational and management controls in an Information system include the following aspects:
- 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 the accounting and financial systems, for example, the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.
- (b) Data processing controls are given as follows:
- *Run-to-run totals*: These help in verifying data that is subjected 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.
 - *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 up dated 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.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- *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.
- (c) Auditors' role in application software acquisition/selection process is given as follows:
- To highlight risks before a vendor contract or a software agreement contract is signed.
 - Ensure that the decision to acquire software should flow through 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/her 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.
- (d) Implementation and operation of controls in a system involves the following five costs:
- (i) *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.
 - (ii) *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
 - (iii) *Correction costs:* If a control has operated reliably in signalling an error or irregularity, the cost associated with the correction of error or irregularity is termed as Correction Cost.
 - (iv) *Failure cost:* If a control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses, which is termed as Failure Cost.

FINAL EXAMINATION :MAY, 2011

- (v) *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.

23. (a) Systematic risks:

These are unavoidable risks; constant across majority of technologies and applications. For example the probability of power outage is not dependant on the industry but is dependant on external factors. Systematic risks would remain, no matter 'what technology is used'. Thus effort to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Systematic risks can be reduced by designing management control process and does not involve technological solutions. For example, the solution to non availability of consumable is maintaining a high stock of the same. Thus a systematic risk can be mitigated not by technology but by management process. Hence, one would not make any additional payment for technological solution to the problem. That means there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

Unsystematic risks:

These are the risks, which are peculiar to the specific applications or technology. One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system. For example, one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. Thus by making additional investment one can mitigate these unsystematic risks.

(b) Delphi Approach:

This approach was first used by the Rand Corporation for obtaining a consensus opinion. Here, a panel of experts is appointed. Each expert gives his opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

Scoring Approach:

In the Scoring approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

(c) [Section 7] Retention of Electronic Records:

- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
 - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
 - (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
 - (c) the details, which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

However, This clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules, regulation etc. in Electronic Gazette.

- 24. (a)** The methodology for developing a business continuity plan emphasizes on the following:
- (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
 - (ii) Obtaining commitment from appropriate management to support and participate in the effort;
 - (iii) Defining recovery requirements from the perspective of business functions;
 - (iv) Documenting the impact of an extended loss to operations and key business functions;
 - (v) Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
 - (vi) Selecting business continuity teams that ensure the proper balance required for plan development;
 - (vii) Developing a business continuity plan that is understandable, easy to use and maintain; and
 - (viii) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

FINAL EXAMINATION :MAY, 2011

- (b) 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.
- (c) If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover the following issues:
- how soon the site will be made available subsequent to a disaster,
 - the number of organizations that will be allowed to use the site concurrently in the event of a disaster,
 - the priority to be given to concurrent users of the site in the event of a common disaster,
 - the period during which the site can be used,
 - the conditions under which the site can be used.
 - the facilities and services the site provider agrees to make available, and
 - what controls will be in place and working at the off-site facility.
25. (a) To qualify for a true ERP solution, a system has to possess the following features:
- **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.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- **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) The detailed controls and objectives of access control are as follows:
- *Business requirement for access control:* To control access to information,
 - *User access management:* To prevent unauthorized access to info systems,
 - *User responsibilities:* To prevent unauthorized user access,
 - *Network access control:* To protect of networked services,
 - *Operating system access control:* To prevent unauthorized computer access,
 - *Application Access Control:* To prevent unauthorized access to information held in information systems,
 - *Monitoring System Access and use:* To detect unauthorized activities, and
 - *Mobile Computing and teleworking:* To ensure information security when using mobile computing & teleworking facilities.
- (c) **[Section 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security:**
- (1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
 - (2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
 - (3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
 - (4) Any intermediary who intentionally or knowingly contravenes the provisions of sub- section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

FINAL EXAMINATION :MAY, 2011

- (d) Major tasks that are to be performed during the post-implementation of an ERP package are given as follows:
- To develop the new job descriptions and organization structure to suit the post ERP scenario;
 - To determine the skill gap between existing jobs and envisioned jobs;
 - To assess training requirements, and create and implement a training plan;
 - To develop and amend HR, financial and operational policies to suit the future ERP environment; and
 - To develop a plan for workforce logistics adjustment.