COMPILATION

OF

SUGGESTED ANSWERS

FINAL COURSE

(NOVEMBER, 2003 – NOVEMBER, 2014)

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

BOARD OF STUDIES

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

(Set up by an Act of Parliament)

NEW DELHI

The Suggested Answers published in this volume do not constitute the basis for evaluation of the students' answers in the examinations. The answers are prepared by the Faculty of the Board of Studies with a view to assist the students in their education. While due care is taken in preparation of the answers, if any errors or omissions are noticed, the same may be brought to the attention of the Director of Studies. The Council of the Institute is not responsible in any way for the correctness or otherwise of the answers published therein.

Website	:	www.icai.org
Department/Committee	:	Board of Studies
E-mail	:	bosnoida@icai.org
Price	:	
ISBN No.	:	
Published by	:	The Publication Department on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi- 110 002, India.
Printed by	:	

Paper -6: Information Systems Control and Audit

Statement indicating chapter-wise distribution of past twenty one examination questions

Term of Examination	Chapter - 1: Concepts of Governance and Management of Information Systems	Chapter - 2: Information Systems Concepts	Chapter - 3: Protection of Information Systems	Chapter - 4: Business Continuity Planning and Disaster Recovery Planning	Chapter - 5: Acquisition, Development and Implementation of Information Systems	Chapter - 6: Auditing of Information Systems	Chapter – 7: Information Technology Regulatory Issues	Chapter – 8: Emerging Technolo-gies	Case Studies
Nov 2003		2 (b)- (i) & (iii), 7 (a)			3 (b), 4 (a), 4 (b)	1 (a), 1 (b)			
May 2004			6 (a)		2 (a), 2 (b)	7 (b), 7 (d)			
Nov 2004					4 (c), 7 (d)	1 (a)	1 (b)		
May 2005		2 (b), 2 (c)	2 (a)	5 (a)	4 (b), 5 (b), 5 (c), 7 (b)		1 (b)		
Nov 2005		3 (a)			2 (c), 3 (b), 7 (d)	5 (b)			
May 2006		1 (c), 2 (a)	1 (d), 6 (a)		3 (a), 4 (c)	5 (a), 6 (b)			
Nov 2006		2 (a)	1 (c)			1 (b), 7 (b)			
May 2007		3 (b), 6 (c)	1 (b)		5 (a), 7 (a), 7 (b)				
Nov 2007		2 (b), 6 (c)	2 (a)		1 (d), 4 (a), 4 (b)		7 (a)		
May 2008		2 (b), 4 (b)	4 (c)		3 (a), 5 (a), 6 (b), 7 (a)				
Nov 2008	5 (a)	1 (b), 2 (b), 2 (c),	3 (a), 4 (b)	6 (a), 6 (b), 6 (c), 7 (d)	2 (a), 3 (b)		1 (c)		
Jun 2009			5 (b)		2 (a), 2 (c)		6 (c), 7 (d)		
Nov 2009		2 (a)	4 (c)		5 (b)		2 (d), 5 (a)		

May 2010		4 (c)		3 (b)	2 (b), 5 (d)	4 (a)	4 (b)		1 (a) & (d)
Nov 2010		7 (c)	3 (c)		6 (a), 6 (b), 7 (a)				1 (a), (b) & (d)
May 2011		3 (b), 5 (b), 7 (a)		3 (c)	6 (a)	6 (b)	7 (d)		1 (a) &(d)
Nov 2011		2 (a)	6 (b), 7 (d)	4 (a)	2 (b), 3 (b), 7 (b)	4 (c), 5 (b)			1 (a) & (d)
May 2012		3 (b), 5 (c)			3 (c), 7 (a)	6 (b)	2 (c), 5 (b), 7 (e)		1 (a), (c) & (d)
Nov 2012		2 (b), 2 (c)	2 (a)	6 (b), 7 (c)	5 (b), 6 (a)	3 (b)			1 (a) & (d)
May 2013	7 (c)	2 (c), 3 (b)	5 (c)		2 (a), 2 (b)	3 (a), 4 (a)	6 (b)		1 (a) & (b)
Nov 2013		2 (a), 6 (b)	3 (a), 5 (b)	3 (b), 7 (c)	2 (b), 7 (e)	4 (b)			1 (a), (b) & (c)

CONTENTS

1

Concepts of Governance and Management of Information Systems

Question 1

Explain the following terms with reference to Information Systems:

(i) Risk

(ii) Threat

(iii) Vulnerability

Or

Risk, Vulnerability and Threat ***(4 Marks, November 2014)***

(iv) Exposure

(v) Attack ***(10 Marks, November, 2008)***

Answer

(i) Risk: Risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset. Information systems can generate many direct and indirect risks which lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by 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 organizations; and external factors such as legislative, legal and regulatory requirements or technological developments.

(ii) Threat: Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a threat. A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat has capability to attack on a system with intent to harm.

(iii) Vulnerability: It is the weakness in the system safeguards that exposes the system to threats. It may be weakness in an information system, cryptographic system, internal controls etc. that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.

(iv) Exposure: It is the extent of loss the organization has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy, loss of resources.

(v) Attack: An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional act, usually an external act that has the intent of exploiting vulnerability in the targeted software or system.

Question 2

Write short note on following:

(a) Risk Assessment ***(4 Marks, May 2013)***

(b) *COBIT 5 Enablers* ***(4 Marks, May 2014)***

(c) *Internal Controls as per COSO* ***(4 Marks, November 2014)***

Answer

(a) Risk Assessment: A risk assessment activity can provide an effective approach, which acts as the foundation for avoiding the disasters. Risk assessment is also termed as a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well-tested contingency plan. In addition, Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan.

Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritize applications, identify exposures and develop recovery scenarios.

(b) COBIT 5 framework describes seven categories of enablers, which are given as follows:

(i) Principles, policies and frameworks are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.

(ii) Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.

(iii) Organizational structures are the key decision-making entities in an enterprise.

(iv) Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.

(v) Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.

(vi) Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

(vii) People, skills and competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

(c) As per COSO, Internal Control is comprised of five interrelated components:

- **Control Environment:** For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.
- **Risk Assessment:** Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.
- **Control Activities:** Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.
- **Information and Communication:** Associated with control activities are information and communication systems. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.
- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

Question 3

What do you understand by IT Governance? Write any three benefits of IT Governance.

(4 Marks, November 2014)

Answer

IT Governance: IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.

Benefits of IT Governance

- Increased value delivered through enterprise IT;
- Increased user satisfaction with IT services;

- Improved agility in supporting business needs;
- Better cost performance of IT;
- Improved management and mitigation of IT-related business risk;
- IT becoming an enabler for change rather than an inhibitor;
- Improved transparency and understanding of IT's contribution to the business;
- Improved compliance with relevant laws, regulations and policies; and
- More optimal utilization of IT resources.

Question 4

You are appointed by a leading enterprise to assess and to evaluate its system of IT internal controls. What are the key management practices to be followed to carry out the assignment complying with COBIT 5? ***(6 Marks, November 2014)***

Answer

The key management practices complying with COBIT 5 for assessing and evaluating the system of IT internal controls in an enterprise are given as follows:

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
- **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers.
- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self-assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.

- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

2
Information Systems Concepts

Question 1

Describe briefly three levels of Management. ***(3 Marks, November 2003)***

Answer

Three levels of management are briefly discussed below:

- **Strategic level**: Strategic level is defined as a set of management positions that is concerned with developing of organizational missions, objectives and strategies, directing and managing the organization in an integrated manner. Decisions made at this level of organization to handle problems critical to the survival and success of the organization is called strategic decisions. Strategic level also establishes a budget framework under which the various departments will operate.
- **Tactical decisions**: This level lies in the middle of managerial hierarchy. At this level, managers plan, organize, lead and control the activities of other managers. Decisions made at this level, called the tactical decisions, are made to implement strategic decisions. Tactical decisions are relatively short, step-like spot solutions to breakdown strategic decisions into implementable packages**.**
- **Supervisory level**: This is the lowest level in managerial hierarchy. The managers at this level coordinate the work of others who are not themselves managers. At supervisory level, managers are responsible for routine, day-to-day decisions and activities of the organization, which do not require much judgment and discretion. They ensure that specific tasks are carried out effectively and efficiently.

Question 2

Discuss the potential impact of computers and MIS at the top level of Management.

(3 Marks, November 2003)

Answer

The potential impact of computers on top-level management May be quite significant. An important factor, which May account for this change, is the fast development in the area of computer science. It is believed that in future computers would be able to provide simulation models to assist top management in planning their activities. By using sensitivity analysis with

the support of computers, it May be possible to study and measure the effect of variation of individual factors to determine final results. Also, the availability of a new class of experts will facilitate effective communication with computers. Such experts May also play a useful role in the development and processing of models. In brief, potential impact of computers would be more in the area of planning and decision-making.

Futurists believe that in future, top management will realize the significance of techniques like simulation, sensitivity analysis and management science. The application of these techniques to business problems with the help of computers would generate accurate, reliable, timely and comprehensive information to top management. Such information will be quite useful for the purpose of managerial planning and decision-making. Computerized MIS will also influence in the development, evaluation and implementation of a solution to a problem under decision-making process.

Question 3

Write short notes on the following:

(a) Executive Information Systems ***(5 Marks, November 2003)***

(b) Expert systems. ***(5 Marks, May 2004)***

(c) Closed and open systems ***(5 Marks, May 2004)***

(d) Benefits of Expert Systems ***(4 Marks, November 2010)***

(e) *Business applications of Expert systems for Management Support systems*

(4 Marks, May 2011)

Answer

(a) Executive Information System (EIS): It is a tool that is designed to meet the special needs of top-level managers. It provides direct on-line access to relevant information in a useful and navigable format. Relevant information is timely, accurate, and actionable about aspects of a business that are of particular interest to the senior manager. The useful and navigable format of the system means that it is specifically designed to be used by individuals with limited time, limited keyboarding skills, and little direct experience with computers. An EIS is easy to navigate so that managers can identify broad strategic issues, and then explore the information to find the root causes of those issues.

EIS require large amounts of capacity and processing power within both the system and the network. Although most computer systems May contain some of the above characteristics, they can be differentiated from EIS in a number of ways. Most MIS and operational systems are based on transaction processing carried out by a variety of on-line and batched inputs. Unlike the EIS, information is usually presented in numerical or textual form and reporting is by exception, usually in printed report format. Also, EISs tend to be externally-focused, strategically-based systems using both internal and

external data, whereas other computer systems mainly concentrate on internal control aspects of the organization.

An EIS serves many purposes. The primary purpose of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment. Informed managers can ask better questions and make better decisions.

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

Finally, an EIS has a powerful ability to direct management attention to specific areas of the organization or specific business problems. Some managers see this as an opportunity to discipline subordinates.

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

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

(c) **Closed Systems:** A closed system is self-contained and does not interact or make exchange across its boundaries with its environment. Closed systems do not get the feedback they need from the external environment and tend to deteriorate eventually. For example, if a marketing system does not get feedback from the market, its efficiency will gradually continue to decrease.

A relatively closed system is one that has only controlled and well defined inputs and outputs. It is not subject to disturbances from its environment. A computer program can

be taken as an example of relatively closed system because it accepts only previously defined inputs, processes them and provides previously defined outputs.

Open Systems: Open systems actively interact with their environment. Such systems regularly get inputs and give outputs to its environment. These systems are also subject to unknown inputs and environmental disturbances. Open systems are also able to adapt to environmental changes for their survival and growth. Business organization is an example of such system.

(d) Benefits of Expert Systems: Major benefits of expert systems are given as follows:

- Expert Systems preserve knowledge that might be lost through retirement, resignation or death of an acknowledged company expert.
- Expert Systems put information into an active-form so that it can be summoned almost as a real-life expert might be summoned.
- Expert Systems assist novices in thinking the way experienced professionals do.
- Expert Systems are not subjected to such human fallings as fatigue, being too busy, or being emotional.
- Expert Systems can be effectively used as a strategic tool in the areas of marketing products, cutting costs and improving products.

(e) Business applications of Expert Systems for Management Support Systems are given as follows:

(i) **Accounting and Finance:** It provides tax advice and assistance, helping with credit authorization decisions, selecting forecasting models, providing investment advice.

(ii) **Marketing:** It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.

(iii) **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.

(iv) **Personnel:** It is useful in assessing applicant qualifications, giving employees assisting at filling out forms.

(v) **General Business:** It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

Question 4

"A decision support system supports the human decision-making process rather than providing a means to replace it". Justify the above statement by stating the characteristics of decision support system. ***(5 Marks, May 2005)***

Or

What is Decision Support System? Briefly explain three characteristics of Decision Support System. ***(5 Marks, November 2008)***

Or

What is Decision Support System? Discuss its characteristics in brief. ***(6 Marks, May 2012)***

Answer

A decision support system (DSS) is defined as a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own way. A DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enables them to generate the information required by them in making decisions. The DSS are characterized by following three properties:

(i) **Semi-structured / Unstructured decisions –** Structured decisions are those that are easily made from a given set of inputs. Unstructured decisions and semi-structured decisions are decisions for which information obtained from a computer system is only a portion of the total knowledge needed to make the decision. The DSS is particularly well adapted to help with semi-structured / unstructured decisions. In DSS, the problem is first defined and formulated. It is then modeled with DSS software. The model is run on the computer to provide results. The modeler, in reviewing these results, might decide to completely reformulate the problem, refine the model, or use the model to obtain other results.

(ii) **Ability to adapt to changing need –** Semi-structured / unstructured decisions often do not conform to a predefined set of decisions-making rules. Because of this, their decision support system must provide for enough flexibility to enable users to model their own information needs. The DSS designer understands that managers usually do not know in advance what information they need and, even if they do, those information needs keep changing constantly. Thus, rather than locking the system into rigid information producing requirements, capabilities and tools are provided by DSS to enable users to meet their own output needs.

(iii) **Ease of Learning and Use -** Since decision support systems are often built and operated by users rather than by computer professionals, the tools that company possesses should be relatively easy to learn and use. Such software tools employ user-oriented interfaces such as grid, graphics, non-procedural 4GL and easily read documentation. These interfaces make it easier for user to conceptualize and perform the decision making process.

Question 5

Describe the main pre-requisites of a Management Information System, which makes it an effective tool. ***(5 Marks, May 2005)***

Answer

Pre-requisites of an MIS – The following are pre-requisites of an effective MIS:

(i) Database – It is a super file which consolidates data records formerly stored in many data files. The data in database is organized in such a way that access to the data is improved and redundancy is reduced. Normally, the database is subdivided into major information sub-sets needed to run. The database should be user-oriented, capable of being used as a common data source, available to authorized persons only and should be controlled by a separate authority such as DBMS. Such a database is capable of meeting information requirements of its executives, which is necessary for planning, organizing and controlling the operations of the business.

(ii) Qualified System and Management Staff - MIS should be manned by qualified officers. These officers who are experts in the field should understand clearly the views of their fellow officers. The organizational management base should comprise of two categories of officers (i) System and Computer experts and (ii) Management experts. Management experts should clearly understand the concepts and operations of a computer. Their whole hearted support and cooperation will help in making MIS an effective one.

(iii) Support of Top Management - An MIS becomes effective only if it receives the full support of top management. To gain the support of top management, the officer should place before them all the supporting facts and state clearly the benefits which will accrue from it to the concern. This step will certainly enlighten the management and will change their attitude towards MIS.

(iv) Control and Maintenance of MIS – Control of the MIS means the operation of the system as it was designed to operate. Sometimes users develop their own procedures or shortcut methods to use the system, which reduces its effectiveness. To check such habits of users, the management at each level in the organization should device checks for the information system control.

Maintenance is closely related to control. There are times when the need for improvements to the system will be discovered. Formal methods for changing and documenting changes must be provided.

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

- Examining the flexibility to cope with future requirements ;
- Ascertaining the view of the users and designers about the capabilities and deficiencies of the system ;
- Guiding the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

Question 6

What is an Executive Information system ? Discuss its various purposes.

(10 Marks, November 2005)

Or

Explain Executive Information System (EIS). What purpose does it serve?

(5 Marks, November 2008)

Answer

An Executive Information System (EIS) is a tool that provides direct online access to relevant information in a useful and navigable format. Relevant information is timely, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager. The useful and navigable format of the system means that it is specifically designed to be used by individuals with limited time, limited key boarding skills and little direct experience with computers. An EIS is quite easy to navigate so that mangers can identify broad strategic issues and then explore the information to find the root causes of those issues.

Executive Information Systems can be used for wide range of applications. In government, EIS have been constructed to track data about ministerial correspondence, case management, workers' productivity, finances and human resources etc. EIS have also been used to monitor information about competitors in the news media and data bases of public information etc.

EIS require large amounts of capacity and processing power within both the system and the network since information is in summary format by pictorial or graphical means. However, EIS has the facility to "drill down" to other levels of information to see the details. The ability to manipulate data, to project "what if" outcomes and to work with modeling tools. Within the system are also evident in EIS.

Purposes of EIS:

(i) The primary purpose of an EIS is to support managerial learning about an organization, its work processes and its interaction with the external environment. Informed managers can ask better questions and make better decisions.

(ii) Second purpose for an EIS is to allow timely access to information. All of the information contained in an EIS can typically be obtained by a manager through traditional methods. However, the resources and time required to manually compile information in a wide variety of formats and in response to ever changing requirements often inhibit managers from obtaining this information. Often, by the time a useful report can be compiled, the strategic issues facing the manager change, and the report cannot be used. Timely access also influences learning. When a manger obtains the answer to a question, that answer typically sparks other related questions in the manger's mind. This way learning cycle continues unbroken.

(iii) Third purpose of an EIS is commonly misperceived. An EIS has a powerful ability to direct management attention to specific areas of the organization or specific business problems. Some managers look upon this as an opportunity to discipline subordinates.

(iv) Sometimes misaligned reporting systems can result in inordinate management attention to things that are not so important. An EIS system can provide information that is actually important and represents a balanced view of the organization's objectives.

Question 7

Discuss the limitations of the Management Information system. ***(5 Marks, May 2006)***

Or

What are major limitations of MIS? Explain in brief. ***(4 Marks, November 2012)***

Answer

Major Limitations of MIS are given as follows:

- The quality of the outputs of MIS is basically governed by the quality of input and processes.
- MIS is not a substitute for effective management, which means that it cannot replace managerial judgment in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS May not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives or senior management.
- MIS is less useful for making non-programmed decisions. Such decisions are not routine and thus require information, which May not be available from existing MIS.
- The effectiveness of MIS is reduced in enterprises, where the culture of hoarding information and not sharing with other is prevalent.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

Question 8

What do you mean by Information? Describe the important characteristics of information, which makes it useful to the organization. ***(10 Marks, May 2006)***

Or

Define the term "Information". Discuss various important attributes that are required for useful and effective information. ***(8 Marks, November 2011)***

Answer

Information: Technically, information means processed data that have been put into a meaningful and useful context. Data consists of facts, values or results, and information is the result of relation between data e.g. in a spread sheet student name, roll number and marks obtained in science and arts subjects represents data whereas the graph that shows the percentage of students, who acquired more than 80% in science subjects and 65% in arts subjects represents information. Information May be represented in the form of text, graph, pictures, voice, videos etc.

Mere collection of data is not information and mere collection of information is not knowledge. Information relates to description, definition, or perspective (what, who, when, where). Information is essential because it adds knowledge, helps in decision making, analyzing the future and taking action in time. Information products produced by an information system can be represented by number of ways e.g. paper reports, visual displays, multimedia documents, electronic messages, graphics images, and audio responses.

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

- **Availability –** It is a very important aspect of information. Information is useless if it is not available at the time of need.
- **Purpose/Objective –** Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data. Depending upon the activities in an organization the Information communicated to people has a purpose. The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.
- **Mode and format –** The modes of communicating information to humans should be in such a way that it can be easily understand by the people. The mode May be in the form of voice, text or a combination of these two. Format also plays an important role in communicating the idea. It should be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information, different formats can be used e.g. diagrams, graphs, curves are best suited for representing statistical data. Format of information should be simple, relevant and should highlight important points but should not be too cluttered up.
- **Current/Updated –** The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed intervals of time so that the current

score will be available. Similar is the case with broker who wants the latest information about the stock market.

- **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. For example- information available from internet site should be available at a click of mouse, and one should not have to wait for it for an hour.
- **Frequency –** The frequency with which information is transmitted or received affects its value. For example- weekly reports of sales show little change as compared to the quarterly reports and contribute less for assessing salesman capability.
- **Completeness and Adequacy –** The information provided should be complete and adequate in itself because only complete information can be used in policy making. For example-the position of student in a class can be found out only after having the information of the marks of all students and the total number of students in a class.
- **Reliability –** 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 the information is reliable.
- **Validity –** It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee does not support evaluating his performance.
- **Quality –** It means the correctness of information. For example, the correct status of inventory is highly required.
- **Transparency –** It is essential in decision and policy making. For example, giving only total amount of advances does not give true picture of utilization of funds for decision about future course of action; rather deposit-advance ratio May be more transparent information as it gives information relevant for decision making.
- **Value of information –** It is defined as 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.

Question 9

State the factors to be considered for designing an effective Management Information System.

(10 Marks, November 2006)

OR

What do you understand by MIS? Discuss major characteristics of an effective MIS.

OR

Describe any six characteristics of an effective management information system.

(6 Marks, November 2013)

Answer

Management Information Systems (MIS): MIS has been defined by Davis and Olson as "An integrated user-machine system designed for providing information to support operational control, management control and decision making functions in an organization". Another notable definition of MIS is **"***MIS is a computer based system that provides flexible and speedy access to accurate data".*

MIS support managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill organizational goals. Nature of MIS at different levels has different flavors and they are available in the form of reports, tables, graphs and charts or in presentation format using some tools. MIS at the top level is much more comprehensive but is condensed or summarized compared to the information provided to those at middle level management. MIS can help in making effective, structured reports relevant for decisions of day-to-day operations. These reports and displays can be made available on demand, periodically or whenever exceptional conditions occur.

Characteristics of an effective MIS: Major characteristics of an effective MIS are given as follows:

- **Management Oriented:** It means that efforts for the development of the Information System should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only but May also meet the information requirements of middle level or operating levels of management.
- **Management Directed:** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote sufficient amount of their time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- **Integrated:** The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are to be tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.
- **Common Data Flows:** It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This

eliminates duplication in data collections, simplifies operations and produces an efficient information system.

- **Heavy Planning Element:** An MIS usually takes one to three years and sometimes even longer to get established firmly within a company. Therefore, a MIS designer must be present while development of MIS and should consider future enterprise objectives and requirements of information as per its organization structure.
- **Sub System Concept:** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time in a phased plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- **Common Database:** Database is the mortar that holds the functional systems together. It is defined as a "super-file", which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
- **Computerized:** Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in MIS.

Question 10

"Decision support systems are widely used as part of an Organization's Accounting Information system". Give examples to support this statement. ***(10 Marks, May 2007)***

OR

Discuss various examples of DSS in Accounting.

Answer

DSSs are widely used as a part of an organization's Accounting Information System. The complexity and nature of decision support systems vary. Many are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Below are several illustrations:

- **Cost Accounting System:** The health care industry is well known for its cost complexity. Managing costs in this industry requires controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help health care organizations calculate product costs for individual procedures or services. Decision support systems can accumulate these product costs to calculate total costs per patient. Health care managers many combine cost accounting decision support systems

with other applications, such as productivity systems. Combining these applications allows managers to measure the effectiveness of specific operating processes. One health care organization, for example, combines a variety of decision support system applications in productivity, cost accounting, case mix, and nursing staff scheduling to improve its management decision making.

- **Capital Budgeting System:** Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. One decision support system designed to support decisions about investments in automated manufacturing technology is Auto Man, which allows decision makers to consider financial, nonfinancial, quantitative, and qualitative factors in their decision-making processes. Using this decision support system, accountants, managers, and engineers identify and prioritize these factors. They can then evaluate up to seven investment alternatives at once.
- **Budget Variance Analysis System:** Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized decision support system to generate monthly variance reports for division comptrollers. The system allows these comptrollers to graph, view, analyze, and annotate budget variances, as well as create additional one-and five-year budget projections using the forecasting tools provided in the system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.
- **General Decision Support System:** As mentioned earlier, some planning languages used in decision support systems are general purpose and therefore have the ability to analyze many different types of problems. In a sense, these types of decision support systems are a decision-maker's tools. The user needs to input data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called *Expert Choice***.** This program supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The decision support system then asks the user to compare decision variables with each other. For instance, the system might ask the user how important cash inflows are versus initial investment amount to a capital budgeting decision. The decision maker also makes judgments about which investment is best with respect to these cash flows and which requires the smallest initial investment. Expert Choice analyzes these judgments and presents the decision maker with the best alternative.

Question 11

Differentiate between open and closed systems. ***(5 Marks, May 2007)***

Answer

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

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

Question 12

System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly. ***(10 Marks, November 2007)***

Answer

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

(i) Transaction processing systems

(ii) Management information systems

(iii) Decision support systems

(iv) Executive information systems

(v) Expert systems.

Three of the above categories are discussed largely below:

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

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

needed for the purpose. In turn, the information systems can be developed so that reports are prepared regularly to support these recurring decisions.

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

Question 13

Briefly explain the principles to guide the design of measures and indicators to be included in EIS. ***(5 Marks, November 2007)***

OR

'There is a practical set of principles to guide the design of measures and indicators to be included in an EIS'. Explain those principles in brief.

Answer

The principles to guide the design of measures and indicators to be included in an EIS are given as follows:

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

- EIS information must be available in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential be part of EIS.
- EIS measures must evolve to meet the changing needs of the organization.

Question 14

Describe the main prerequisites of a MIS which makes it an effective tool. Explain the major constraints in operating it. ***(10 Marks, May 2008)***

Answer

The main pre-requisites of an effective MIS are as follows:

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

- ♦ The database is sub-divided into major information subsets needed to run a business wherein each subsystem utilizes same data and information kept in same file to satisfy its information needs.
- ♦ It is user-oriented.
- ♦ It is capable of being used as a common data source, to various users, helps in avoiding duplication of efforts in storage and retrieval of data and information.
- ♦ It is available to authorized persons only.
- ♦ It is controlled by a separate authority established for the purpose, known as Data Base Management System (DBMS).
- ♦ The maintenance of data in database requires computer hardware, software and experienced computer professionals.

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

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

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

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

Their whole hearted support and cooperation will help in making MIS an effective one.

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

(v) **Evaluation of MIS:** The evaluation of MIS should take into account the following points:

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

Constraints in operating MIS

Major constraints which come in the way of operating an information system are:

(1) Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing an operating system.

(2) Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon.

(3) Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.

(4) Non-availability of cooperation from staff in fact is a crucial problem. It should be handled tactfully. Educating the staff by organizing lectures, showing films, training on system and utility of the system May solve this problem.

(5) There is high turnover of experts in MIS. Turnover in fact arises due to several factors like pay packet, promotion chances, future prospects, behaviour of top ranking managers etc.

(6) Difficulty in quantifying the benefits of MIS, so that it is easily comparable with cost.

Question 15

Briefly discuss four basic components of Decision Support System. ***(5 Marks, May 2008)***

Answer

A decision support system has the following components:

(i) **The User:** The user of a decision support system is usually a manager with an unstructured or semi-structured problem to solve. Users do not need a computer background to use a decision support system for problem solving. The most important knowledge is a thorough understanding of the problem and the factors to be considered in finding a solution. A user does not need extensive education in computer programming in part because a special planning language performs the communication function within the decision support system.

(ii) **One or more databases:** Decision support systems include one or more databases which contain both routine and non-routine data from both internal and external sources. The data from external sources include data about the operating environment surrounding an organization. Decision support system users May construct additional database themselves. Some of the data May come from internal source.

(iii) **A planning language:** Two types of planning languages that are commonly used in decision support system are (1) general purpose planning languages and (2) special purpose planning languages. General purpose planning languages allow users to perform many routine tasks like-retrieving various data from a database or performing statistical analysis. The languages in most electronic spreadsheets are good example of general purpose planning languages. These languages enable the user to tackle a broad range of budgeting, forecasting and other worksheet oriented problems. Special purpose planning languages are more limited. Some statistical languages, such as SAS, SPSS and Minitab are examples of special purpose planning languages.

(iv) **Model Base:** The model base is the "brain" of the decision support system because it performs data manipulation and computations with the data provided to it by the user and the database. There are many types of model bases but most of them are custom-developed models that do some type of mathematical functions. The analysis provided by the routine in the model base is the key to supporting the user's decision.

Question 16

Identify and justify the type of each one of the following systems based on how they perform within an environment and/or certainty/ uncertainty:

i. Marketing system

ii. Communication system

iii. Manufacturing system

iv. Pricing system

v. Hardware-Software system. ***(5 Marks, November 2009)***

Answer

	System Type	Justification
(i) Marketing system	Open System	The marketing system plays a pivotal role in the running of a business in the competitive environment. The objective of the system is to maximize customer satisfaction by providing a free interactive environment. The system takes input/feedbacks and facilitates the outcomes as products of the company and to create new customers.
(ii) Communication System	Open System	The communication system in a organization is a point of contact to balance the external influence and render its services to the customers. The system interacts freely with its environment by taking input and returning output.
(iii) Manufacturing System	Closed System	This system is in place to meet a particular objective. It does not interact neither with the environment nor changes with the change in the environment. A manufacturing unit is completely isolated from its environment for its operation.
(iv) Pricing System	Probabilistic and Open System	The system has a probable behavior and interacts freely with its environment by taking inputs and returning outputs. The pricing system is a dynamic one which influences the form of profit and goodwill of an organization.
(v) Hardware-Software System	Closed Deterministic System	Since the interaction among the parts of the system is known with certainty and does not interact with the environment and does not change with the change in the environment. Here the requirements of the hardware and software inventory are known with certainty. The operational state of these systems is in a predictable manner.

Question 17

Discuss some of the important advantages of Information Systems in business.

(5 Marks, May 2010)

Answer

Following are some of the important implications of Information Systems in business:

- Information Systems help managers in efficient decision-making to achieve organizational goals.
- An organization will be able to survive and thrive in a highly competitive environment on the strength of a well-designed Information system.
- Information Systems help in making right decision at the right time i.e. just on time.
- A good Information System May help in generating innovative ideas for solving critical problems.
- Knowledge gathered though Information systems 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.

Question 18

What are the characteristics of Executive Information System? ***(4 Marks, May 2011)***

OR

What is meant by EIS? What are its characteristics? ***(6 Marks, November 2012)***

Answer

Executive Information Systems (EIS): It is sometimes referred to as an Executive Support System (ESS) too. It serves the strategic level i.e. top level managers of the organization. ESS creates a generalized computing and communications environment rather than providing any preset applications or specific competence.

Characteristics of EIS: Major Characteristics of an EIS are given as follows:

- EIS is a Computer-based-information system that serves the information need of top executives.
- EIS enables users to extract summary data and model complex problems without the need to learn query languages statistical formulas or high computing skills.
- EIS provides rapid access to timely information and direct access to management reports.
- EIS is capable of accessing both internal and external data.
- EIS provides extensive online analysis tool like trend analysis, market conditions etc.
- EIS can easily be given as a DSS support for decision making.

Question 19

Discuss important characteristics of Computer based Information Systems in brief.

(4 Marks, May 2011)

Answer

Major characteristics of Computer based Information Systems are given as follows:

- All systems work for predetermined objectives and the system is designed and developed accordingly.
- In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
- If one subsystem or component of a system fails; in most of the cases, the whole system does not work. However, it depends on 'how the subsystems are interrelated'.
- The way a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system.
- The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.

Question 20

Discuss the constraints in operating a MIS. ***(4 Marks, May 2012)***

OR

Write a short note on Limitations of MIS. ***(4 Marks, November 2012)***

'There are various constraints, which come in the way of operating an MIS'. Explain any four such constraints in brief.

Answer

Four major constraints, which come in the way of operating an MIS, are given as follows:

- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing a system, which operates properly. 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 which sub-system of MIS should be installed and operated first. The criteria, which should guide the experts, depend its need and importance.
- Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is no-standardized.

- Non-cooperation from staff is a crucial problem, which should be handled tactfully. This can be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some staff should also be involved in the development and implementation of the system to buy-in their participation.

Question 21

Explain any four features of Electronic Mail. ***(4 Marks, November 2012)***

Answer

Major features of an Electronic Mail are given as follows:

- **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 the use of paper/s 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 the branches of a bank using Email resulting in a lot of saving of papers. 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. 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 for 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 proving to be very helpful not only for formal communication but also for informal communication within the business enterprise.

Question 22

How does Executive Information System differs from Traditional Information System?

(4 Marks, May 2013)

Answer

Executive Information Systems differs from Traditional Information Systems in many ways. The following table presents the difference on various related dimensions:

Dimensions of Difference	Executive Information System	Traditional Information System
Level of management	For top or near top executives	For lower staff
Nature of Information Access	Specific issues/problems and aggregate reports	Status reporting
Nature of information provided	Online tools and analysis	Offline status reporting
Information Sources	More external, less internal	Internal
Drill down facility to go through details at successive levels	Available	Not available
Information format	Text with graphics	Tabular
Nature of interface	User-friendly	Computer-operator generated

Question 23

What is an Expert System? List the properties which an application should possess to qualify for Expert System development. ***(6 Marks, May 2013)***

Or

What do you mean by an Expert System? Briefly explain some of the properties that potential applications should possess to qualify for an expert system development.

(6 Marks, November 2014)

Answer

Expert System: An Expert System is highly developed Decision Support System (DSS) that utilizes the knowledge generally possessed by an expert to solve a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – how much can be invested. Does the client have any preferences regarding specific types of securities?

Major properties that an application should possess to qualify for Expert System development are given as follows:

- **Availability**: One or more experts are capable of communicating 'how they go about solving the problems to which the Expert System will be applied'.
- **Complexity**: Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing.
- **Domain**: The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.
- **Expertise**: Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- **Structure**: The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

Question 24

Define Transaction Processing System (TPS). List out the salient features of a TPS.

(6 Marks, November 2013)

Answer

Transaction Processing System (TPS): TPS at the lowest level of management is an information system that manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use. TPS records and manipulates transaction data into usable information.

The salient features of a TPS are given as follows:

- **Large volume of data:** As TPS is transaction – oriented, it generally consists large volumes of data and thus requires greater storage capacity. Their 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 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.
- **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.

Question 25

An owner of a small local store is currently using manual system for his day to day business activities viz. purchase, sales, billing, payments receipts etc. In the last few years, turnover of the store is increased manifold and now it has become increasingly difficult to handle all these activities manually. You being an IT expert and his auditor, are requested to suggest which operation support system will be most suitable for him. Also advise him what activities can be performed by the proposed system and what are major limitation of it. ***(6 Marks, May 2014)***

Answer

In the given scenario, we would suggest the owner of the local store to go for Transaction Processing System (TPS), which will be the most suitable option for him. Because TPS at the lowest level of management is an information system that manipulates data from business transactions efficiently and if properly computerized, TPS provides speed and accuracy too. Various day-to-day business activities such as sales, purchase, production, billing, payments or receipts involves transactions and these transactions are to be organized and manipulated to generate various information products for external use.

Following are the major activities, which can be performed by the proposed TPS:

- Capturing data to organize in files or databases;
- Processing of files / databases using application software;
- Generating information in the form of reports;
- Processing of queries from various quarters of the organization.

A TPS May follow periodic data preparation and batch processing (as in payroll application) or on-line processing (as in inventory control application). In industries and business houses, now-a-days, on-line approach is preferred as it provides information with up-to-date status.

However, the people involved in TPS, usually are not in a position to take any management decision. This is the major limitation of it.

Question 26

Modem business uses Information Technology to carry out basic functions including systems for sales, advertisement, purchase, Management reports etc. Briefly discuss some of the IT tools crucial for business growth. ***(6 Marks, November 2014)***

Answer

(a) Some of the IT tools crucial for business growth are as follows:

- **Business Website –** By having a website, enterprise/business becomes reachable to large amount of customers. In addition, it can also be used in an advertisement, which is cost effective and in customer relationship management.
- **Internet and Intranet –** Time and space are no obstacles for conducting meeting of people working in a team from multiple locations, or with different vendors and companies. Intranet is system that permits the electronic exchange of business data within an organization, mostly between managers and senior staff. E-commerce among partners (suppliers, wholesalers, retailers, distributors) using intranets, e-mail etc. provides new platform to the business world for conducting business in a faster and easier way.
- **Software and Packages –** DBMS, data warehousing, data mining tools, knowledge discovery can be used for getting information that plays important role in decision making that can boost the business in the competitive world. ERP is one of the latest high-end solutions that streamlines and integrates operation processes and information flows in the company to synergize major resources of an organization.
- **Business Intelligence –** Business Intelligence (BI) refers to applications and technologies that are used to collect; provide access and analyze data and information about companies operations. Some BI applications are used to analyze performance or internal operations e.g. EIS (executive information system), business planning, finance and budgeting tools; while others are used to store and analyze data e.g. Data mining, Data Warehouses, Decision Support System etc. Some BI applications are also used to analyze or manage the human resources e.g. customer relationship and marketing tools.
- **Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc. –** Webcam, microphone etc. are used in conducting long distance meeting. Use of computer systems, printer, and scanner increases accuracy, reduce processing times, enable decisions to be made more quickly and speed up customer service.

3

Protection of Information Systems

Question 1

Explain in brief information security and its importance. ***(10 Marks, May 2004)***

OR

What is "Information Security"? State the core principles of Information Security.

(10 Marks, May 2005)

Answer

Information security: Security relates to the protection of valuable assets against loss, disclosure, or damage. Securing valuable assets from threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is commonly understood and implemented by most organizations. However, security must be expanded to include logical and other technical safeguards such as user identifiers, passwords, firewalls, etc. which are not understood nearly as well by organizations as physical safeguards. In organizations where a security breach has been experienced, the effectiveness of security policies and procedures has to be reassessed.

This concept of security applies to all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information is protected against harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure. The protection is achieved through a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, firewalls, etc.

The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity".

For any organization, the security objective is met when

- information systems are available and usable when required (availability),
- data and information are disclosed only to those who have a right to know it (confidentiality),
- data and information are protected against unauthorized modification (integrity).

Importance of Information Security: In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. Organizations depend on timely, accurate, complete, valid, consistent, relevant and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment.

Today, there are many direct and indirect risks relating to the information systems. These risks have led to gap between the need to protect systems and the degree of protection applied. This gap is caused by:

- 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 over more conventional physical attacks against organizations; and
- External factors such as legislative, legal, and regulatory requirements or technological developments;

Security failures May result in both financial losses and / or intangible losses such as unauthorized disclosure of competitive or sensitive information.

Threats to information system May arise from intentional or unintentional acts and May come from internal or external sources. The threats May emanate from, among others, technical conditions (program bugs, disk crashes), natural disasters (fires, floods), environmental conditions(electrical surges), human factors (lack of training, errors, and omissions), unauthorized access (hacking), or viruses. In addition to these, other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.) that can potentially result in a loss of management control and oversight are increasing in significance.

Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss or embarrassment caused by security failures.

Question 2

Define the following computer Fraud and Abuse technique:

(i) Hacking

(ii) Logic time bomb

(iii) Piggy backing

(iv) Spamming

(v) Data diddling. ***(5 Marks, May 2006)***

Answer

(i) Hacking: It refers to unauthorized access to and use of computer system usually by means of a personal computer and telecommunication network.

(ii) Logic time Bomb: It refers to the program that lies idle until some specified circumstance or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.

(iii) Piggy Backing: It refers to tapping into a telecommunications line and latching on to a legitimate user before he logs into the system; legitimate user unknowingly carries perpetrator into the system.

(iv) Spamming: It refers to a situation where the same message is e-mailed to everyone on one or more Usenet news groups or LISTSERV lists.

(v) Data diddling: Changing data before, during or after it is entered into the system in order to delete alter or add key system data is known as data diddling.

Question 3

What do you mean by Information Security policy? Explain the salient features of the Information Security Policy. ***(10 Marks, May 2006)***

Answer

Information Security Policy: Security policy defines acceptable behaviours and the reaction of the organization when such behaviours are violated. The electronic trading, viruses affecting organization's security documents and the misuse of credit cards have increased and this has augmented the need for security management. Also, legislation relating to information technology is becoming more prolific, with many countries enacting laws on issues such as copyright and software privacy, intellectual property and personal data. These commercial, competitive and legislative pressures require the implementation of proper security policies.

A good security policy should suggest procedures and policies that can prevent loses and also help in saving money and increasing productivity. The security policy defines ways in which resources in a computer system May be accessed and used. Security policies might differ depending upon the system under consideration.

Features of Information Security Policy: The security objectives and core principles provide a framework for the first critical step for any organization-developing a security policy. The security policy should support and complement existing organizational policies. The thrust of the policy statement must be to recognize the underlying value of, and dependence on, the information within an organization. The information security policy should describe:

- Importance of information security to the organization

- A statement from the chief executive officer in support of goals and principles of effective information security.
- Specific statements indicating minimum standards and compliance requirements for specific areas.
- Asset classifications.
- Data security
- Personnel security
- Physical, logical and environment security
- Communications security
- Legal, regulatory and contractual security
- System development and maintenance life cycle requirements
- Business continuity planning
- Security awareness, training and education
- Security breach detection and reporting requirements
- Violation enforcement provision
- Definitions of responsibility, accountability for information security and proper separation of duties
- Reporting responsibilities and procedures.

Question 4

Differentiate between General and Application controls. Also mention the broad categories into which the first can be subdivided. ***(5 Marks, November 2006)***

Answer

General controls apply to a wide range of exposures that systematically threaten the integrity of all applications processed within CBIS environment. **Application controls** are focused on exposures associated with specific systems such as payroll, accounts receivable etc. These controls help to ensure the completeness and accuracy of transaction processing, authorization, and validity.

General controls can be subdivided under following headings:

(1) Operating system controls

(2) Data managements Controls

(3) Organizational structure controls

(4) Systems development controls

(5) Systems maintenance controls

(6) Computer Centre security controls

(7) Internet and intranet controls

(8) Personal computers control.

Question 5

Briefly outline the contents of Information Security policy. ***(5 Marks, May 2007)***

OR

State the components of a security policy to protect information system of an organization.

(6 Marks, November 2013)

Answer

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 Compliance; and
- Monitoring and Auditing Requirements.

Aforementioned components are the major contents of a typical security policy. However, the policy is always organization specific and accordingly, a study of the organizations' functions, their criticality and the nature of the information would determine the content of the security policy.

Question 6

What is "Information Security"? Why is it important in any organization? Explain briefly

(10 Marks, November 2007)

Answer

Security refers to the protection of valuable assets against loss, disclosure or damage. "Information Security" covers all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted or retrieved from an electronic medium. It is protected against harm from threats leading to its loss, damage, inaccessibility, integrity or unauthorized disclosure. The protection of these unbreakable assets is achieved by deploying a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, anti-virus, firewalls etc.

In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. In addition, information and the information system and communication that deliver the information are truly pervasive throughout organization – from the user's platform to local and wide area networks to servers to main frame computers. Organizations depend on timely, accurate, complete, valid, consistent, relevant and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment. It is clear that there are not only many direct and indirect benefits from the use of information systems, there are also many risks (direct and indirect) relating to information systems. Most risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by various factors such as (i) widespread use of technology, (ii) interconnectivity of systems, (iii) elimination of distance, time and space etc. (iv) unevenness of technological changes, (v) Devolution of management and control, (vi) Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations, and (vii) External factors such as legislative, legal, and regulatory requirements or technological developments.

Threats to information systems May arise from intentional or unintentional acts and many come from internal or external sources. The threats May emanate from, among others, technical conditions (program bugs, disk crashes), natural disasters (fires, floods), environmental conditions, human factors, unauthorized access or viruses.

Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss or embarrassment caused by security failure. That is why; the organizations have started giving more and more importance towards information security.

Question 7

Define the following computer fraud and abuse technique:

(i) War dialing

(ii) Scavenging

(iii) Cracking

(iv) Internet terrorism

(v) Masquerading. ***(10 Marks, May 2008)***

Answer

(i) War dialing: It relates to programming a computer search for an idle modem by dialing thousands of phone lines. Perpetrator enters the system through idle modem, captures the personal computer attached to the modem, and gain access to the network to which the personal computer is attached.

(ii) Scavenging: Gaining access to confidential information by searching corporate records is termed as scavenging. Scavenging methods range from searching for printouts or carbon copies of confidential information to scanning the contents of computer memory.

(iii) Cracking: Unauthorized access to and use of computer systems, usually by means of a personal computer and a telecommunications network is called cracking. Crackers are hackers with malicious intentions.

(iv) Internet terrorism: Using internet to disrupt electronic commerce and to destroy company and individual communications is referred as internet terrorism.

(v) Masquerading: Under this technique, perpetrator gains access to the system by pretending to be an authorized user and enjoys same privileges as the legitimate user. Fraud messages can be sent to the receiver by using legitimate users identity and thus can prove to be harmful.

Question 8

What do you understand by classification of information? Explain different classifications of information. ***(10 Marks, November 2008)***

Answer

Information classification does not follow any predefined rules. It is a conscious decision to assign a certain sensitivity level to information that is being created, amended, updated, stored, or transmitted. The sensitivity level depends upon the nature of business in an organization and the market influence.

The classification of information further determines the level of control and security requirements. Classification of information is essential to understand and differentiate between the value of an asset and its sensitivity and confidentiality. When data is stored, whether

received, created or amended, it should always be classified into an appropriate sensitivity level to ensure adequate security.

For many organizations, a very simple classification criterion is given as follows:

- **Top Secret:** Highly sensitive internal information (e.g. pending mergers or acquisitions; investment strategies; plans or designs) that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret information has very restricted distribution and must be protected at all times. Security at this level should be the highest possible.
- **Highly Confidential:** Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants, patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organization's operational control without specific authority. Security at this level should be very high.
- **Proprietary:** Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only. Security at this level should be high.
- **Internal Use only:** Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level should controlled but normal.
- **Public Documents:** Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level should minimal.

Question 9

Discuss various types of Information Security polices and their hierarchy.

(5 Marks, November 2008)

OR

Give the hierarchy of Information Security Policies and discuss each one of them.

(4 Marks, November 2011)

Answer

Various types of information security policies are:

- **Information Security Policy –** This policy provides a definition of Information Security, its overall objective and the importance that applies to all users.
- **User Security Policy –** This policy sets out the responsibilities and requirements for all IT

system users. It provides security terms of reference for Users, Line Managers and System Owners.

- **Acceptable Usage Policy –** This sets out the policy for acceptable use of email, Internet services and other IT resources.
- **Organizational Information Security Policy –** This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.
- **Network & System Security Policy –** This policy sets out detailed policy for system and network security and applies to IT department users
- **Information Classification Policy –** This policy sets out the policy for the classification of information
- **Conditions of Connection –** This policy sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

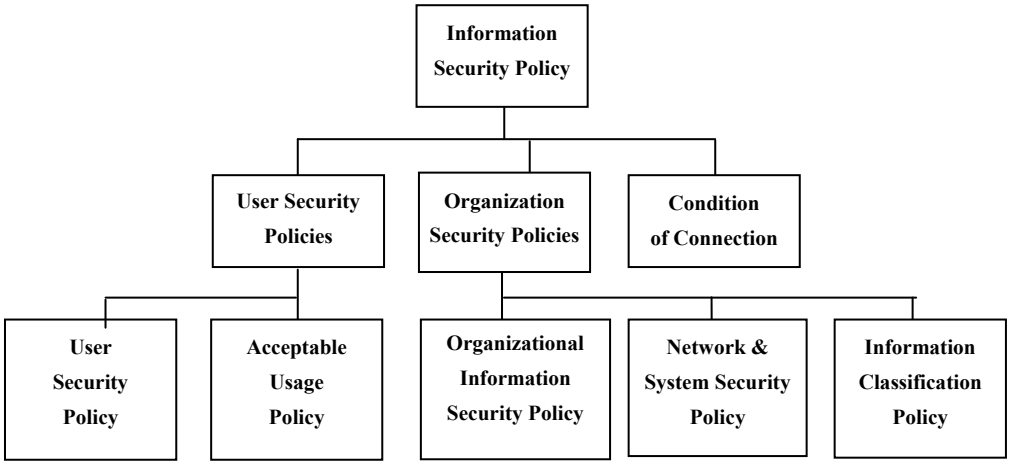

Fig. : The hierarchy of Information Security Policies

Question 10

The Information Security Policy of an organization has been defined and documented as given below:

"Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes."

Discuss Information Security Policy and also identify the salient components that have not been covered in the above policy. ***(5 Marks, June 2009)***

OR

What is Information Security Policy? What are the issues it should address?

(4 Marks, May 2013)

Answer

A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization.

An Information Security Policy addresses many issues such as disclosure, integrity and availability concerns, who May access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls, who owns the information, and authority issues.

Issues to address: This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by an appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities, and
- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy May be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

In the stated scenario of the question, the ISMS Policy of the given organization does not address the following issues:

- Definition of information security,
- Reasons why information security is important to the organization,
- A brief explanation of the security policies, principles, standards and compliance, and
- Reference to supporting documents.

Question 11

Discuss the three processes of Access Control Mechanism, when a user requests for resources. ***(5 Marks, November 2009)***

Answer

Access control mechanism processes the user request for resources in three steps. They are:

- Identification
- Authentication
- Authorization

The access control mechanisms operate in the following sequence:

1. The users have to identify themselves, thereby indicating their intent to request the usage of system resources,
2. The users must authenticate themselves and the mechanism must authenticate itself, and
3. The users request for specific resources, their need for those resources and their areas of usage of these resources.

   The mechanism accesses

   (a) previously stored information about users,

   (b) the resources they can access, and

   (c) the action privileges they have with respect to these resources.

   The mechanism verifies this information against the user entries and it then permits or denies the request.

Identification and Authentication: Users identify themselves to the access control mechanism by providing information such a name, account number, badge, plastic card, finger print, voice print or a signature. To validate the user, his entry is matched with the entry in the authentication file. The authentication process then proceeds on the basis of information contained in the entry, the user having to indicate prior knowledge of the information.

Authorization: There are two approaches to implementing the authorization module in an access control mechanism:

- **Ticket oriented:** In this approach the access control mechanism assigns the users a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user
- **List oriented:** In this approach, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

Question 12

"Once the information is classified on various levels, the organization has to decide about the implementation of different data integrity controls." Do you agree? If yes, explain about data integrity and its policies. ***(8 Marks, November 2010)***

Answer

Yes, we agree with the statement given in the question.

Data integrity is a reflection of the accuracy, correctness, validity and currency of the data. The primary objective in ensuring integrity is to protect the data against erroneous input from authored users.

Major data integrity policies are given as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **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.
- **Offsite Backup Storage:** Backups 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.

Question 13

Write a short note on following:

(a) Locks on Doors with respect to Physical Access Control. ***(4 Marks, November 2011)***

(b) Information System (IS) security objective ***(4 Marks, May 2014)***

(c) Operating System Security ***(4 Marks, November 2014)***

Answer

(a) Locks on Doors with respect to physical access control: Different types of locks on doors for physical security are discussed below:

- **Cipher Locks (combination Door Locks):** The Cipher Lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.

  Cipher Locks are used in low security situations or when a large number of entrances and exits must be usable all the time. More sophisticated and expensive cipher locks can be computer coded with a person's handprint. A matching handprint unlocks the door.

- **Bolting Door Locks:** A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should not be duplicated.

- **Electronic Door Locks:** A magnetic or embedded chip based plastics card key or token May be entered into a sensor reader to gain access in these systems. The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism.

- **Biometric Door Locks:** These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

(b) Information System 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".

For any organization, the security objective comprises three universally accepted attributes, which are given as follows:

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

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

(c) Operating System Security: Operating System Security involves policy, procedure and controls that determine, 'who can access the operating system', 'which resources they

can access', and 'what action they can take'. The following security components are found in secure operating system:

- **Log-in Procedure:** A log-in procedure is the first line of defense against unauthorized access. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized.
- **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.
- **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.
- **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, resource owners in distributed systems May be granted discretionary access control which allows them to grant access privileges to other users.

(b) Operating System Security: Operating System Security involves policy, procedure and controls that determine, 'who can access the operating system', 'which resources they can access', and 'what action they can take'. The following security components are found in secure operating system:

- **Log-in Procedure:** A log-in procedure is the first line of defense against unauthorized access. When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized.
- **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.
- **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

- **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, resource owners in distributed systems May be granted discretionary access control which allows them to grant access privileges to other users.

Question 14

XYZ Ltd. is a large multinational company with offices in many locations. It stores all its data in just one centralized computer centre. It uses Internal Controls in order to asset safeguarding, data integrity, system efficiency and effectiveness. What could be the interrelated components of its Internal Control? Discuss them briefly. ***(6 Marks, November 2012)***

Answer

Internal controls used within XYZ Ltd. May comprise of the following five interrelated components:

- Control environment,
- Risk assessment,
- Control activities,
- Information and communication, and
- Monitoring.

A brief overview of each component is given as follows:

- **Control Environment:** Elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.
- **Risk Assessment:** Elements that identify and analyse the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation.
- **Control Activities:** Elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.
- **Information and Communication:** Elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.
- **Monitoring:** Elements that ensure internal controls operate reliably over time.

Question 15

Explain, briefly, the six categories of controls classified on the basis of nature of IS resources.

(6 Marks, November 2013)

Answer

Six categories of controls classified on the basis of the nature of IS resources are given as follows:

(i) **Environmental Controls:** Controls relating to the housing of IT resources such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc.

(ii) **Physical Access Controls:** Controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, video monitoring etc.

(iii) **Logical Access Controls:** Controls relating to logical access to information resources such as operating systems controls, Application software boundary controls, networking controls, access to database objects, encryption controls etc.

(iv) **IS Operational Controls:** Controls relating to IS operation, administration and its management such as day begin and day end controls, IS infrastructure management, Helpdesk operations etc.

(v) **IS Management Controls:** Controls relating to IS management, administration, policies, procedures, standards' and practices, monitoring of IS operations, Steering committee etc.

(vi) **SDLC Controls:** Controls relating to planning, design, development, testing, implementation and post implementation, change management of changes to application and other software.

Question 16

Describe the various threats to the computerized environment due to cyber crimes.

(6 Marks, May 2014)

Answer

Following are major threats due to cyber-crimes:

- **Embezzlement:** It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.
- **Fraud:** It occurs on account of internal misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud May be committed by someone inside or outside the company.

- **Theft of proprietary information:** It is illegal to obtain of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
- **Denial of service:** An action or series of actions that prevents access to a software system by its intended/authorized users or causes the delay of its time-critical operations or prevents any part of the system from functioning is termed as 'DoS'. There can be disruption or degradation of service that is dependent on external infrastructure. Problems May erupt through internet connection or e-mail service those results in an interruption of the normal flow of information. DoS is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.
- **Vandalism or sabotage:** It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- **Computer virus:** Viruses are hidden fragments of computer codes, which propagate by inserting themselves into or modifying other programs.
- **Others:** Threat includes several other cases such as intrusion, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

Question 17

Explain the various financial control techniques used in information system control.

(6 Marks, May 2014)

Answer

Financial control techniques are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These are numerous; some key techniques are given as follows:

- **Authorization:** This entails obtaining the authority to perform some act typically access to such assets as accounting or application entries.
- **Budgets:** These estimates 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.
- **Cancellation of documents:** This 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 persons simultaneously access an 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.
- **Sequentially numbered documents:** These are working documents with preprinted sequential numbers, which enables 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.

Question 18

Mr. 'X' has opened a new departmental store and all the activities are computerized. He uses Personal Computers (PCs) for carrying out the business activities. As an IS auditor, list the risks related to the use of PCs in the business of Mr. 'X' and suggest any two security measures to be exercised to overcome them. ***(6 Marks, November 2014)***

Answer

Risks related to the use of PCs in the business are as follows:

- Personal computers are small in size and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft of information.
- Pen drives can be very conveniently transported from one place to another, as a result of which data theft May occur. Even hard disks can be ported easily these days.
- PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption, slow operations and system break down etc.
- Segregation of duty is not possible, owing to limited number of staff.
- Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.
- The operating staff May not be adequately trained.

- Weak access control: Most of the log-on procedures become active at the booting of the computer from the hard drive.

The Security Measures that could be exercised to overcome these aforementioned risks are given as follows:

- Physically locking the system;
- Proper logging of equipment shifting must be done;
- Centralized purchase of hardware and software;
- Standards set for developing, testing and documenting;
- Uses of antimalware software; and
- The use of personal computer and their peripheral must have controls.
- Use of disc locks that prevent unauthorized access to floppy disk or pen drive of a computer.

Question 19

As an IS auditor, what are the output controls required to be reviewed with respect to application controls? ***(6 Marks, November 2014)***

Answer

As an IS Auditor, various Output Controls required to be reviewed with respect to Application Controls are as follows:

- **Storage and logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.
- **Logging of output program executions:** When programs used for output of data are executed, these should be logged and monitored; otherwise confidentiality/integrity of the data May be compromised.
- **Spooling/queuing:** "Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user is able to continue working, while the print operation is getting completed.
- **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place. Users must be trained to select the correct printer and access restrictions May be placed on the workstations that can be used for printing.
- **Report distribution and collection controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. A log should be maintained for

reports that were generated and to whom these were distributed. Uncollected reports should be stored securely.

- **Retention controls:** Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced.

Question 20

What are the repercussions of cyber frauds on an enterprise? ***(4 Marks, November 2014)***

Answer

The repercussions of cyber frauds on an enterprise can be viewed under the following dimensions:

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.
- **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
- **Loss of credibility or Competitive Edge:** News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility.
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack May expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.
- **Sabotage:** The above situation May lead to misuse of such information by enemy country.

4

Business Continuity Planning and Disaster Recovery Planning

Question 1

What do you understand by disaster recovery plan? Discuss its various components.

(10 Marks, May 2005)

OR

Explain the various general components of Disaster Recovery Plan. ***(6 Marks, November 2011)***

Answer

Disaster Recovery Plan – The term disaster recovery describes the contingency measures that organizations have adopted at key computing sites to recover from or to prevent any monumentally bad event or disaster. A disaster may result from natural causes such as fire, flood or earthquake etc. or from other sources such as a violent takeover, willful or accidental destruction of equipment or any other act of such catastrophic proportion that the organization could be ruined. The primary objective of a disaster recovery plan is to assure the management that normalcy would be restored in a set time after any disaster occurs, thereby minimizing losses to the organization.

Although each organization would have its own tailored disaster recovery plan, the general components of the plan are as follows:

(1) Emergency Plan – It outlines the actions to be undertaken immediately after a disaster occurs. It identifies the personnel to be notified immediately. It provides guidelines on shutting down equipment, termination of power supply, removal of storage files, and removable discs. It sets out evacuation procedures. It also provides return procedures as soon as the primary facility is ready for operation like backing up data files at off-site, deleting data from disk drives at third party site, relocation of proper versions of backup files etc.

(2) Recovery Plan – This part of disaster recovery plan sets out how the full capabilities will be restored. The following steps may be carried out under this plan:

(i) Inventory of hardware, application systems, system software, documentation etc. must be taken.

(ii) Criticality of application systems to the organization and the importance of their loss must be evaluated. An indication must be given of the efforts and cost involved in restoring the various application systems.

(iii) An application systems hierarchy must be spelt out. This would be used when the management decides to accept a degraded mode of operation.

(iv) Selection of a disaster recovery site must be made. A reciprocal agreement with another organization having compatible hardware and software could be made.

(v) Formal backup arrangement should be made. This should cover the periodical exchange of information between the two sites regarding changes to hardware / software, the time and duration of system availability.

(3) Backup Plan – Organization no matter how physically secure, their systems are always vulnerable to the disaster. Therefore, an effective safeguard is to have a backup of anything that could be destroyed, be it hardware or software. As far as software is concerned, it is necessary to make copies of important programs, data files, operating system and test programs etc. in order to get back into operation before the company can suffer an intolerable loss. Often, the originals are stored at a site that is physically distant from the actual site and where duplicate copies are used for processing. The backup copies must be kept in a place, which is not susceptible to the same hazards as the originals.

(4) Test Plan – Test Plan looks after the testing of DRP and analysis of the result. It identifies deficiencies in the emergency, backup or recovery plan. It contains procedures for conducting DRP testing like:

(i) Paper Walkthrough - It involves critical personnel in the plan's execution, reasoning out what might happen in the event of different disasters.

(ii) Localized Tests - It simulates system crash. This test is performed on different aspects of DRP.

(iii) Full operational test - It is nearer to disaster conditions. Paper walkthrough and localized test should have been conducted before completely shutting down the operation to simulate disasters.

Question 2

Discuss the objectives and goals of Business Continuity planning. ***(5 Marks, November 2008)***

Answer

Objectives of Business Continuity Planning: The primary objective of a business continuity planning is to enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can

resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- Provide for the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimise immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort;
- Identify critical lines of business and supporting functions.

Question 3

What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery? ***(10 Marks, November 2008)***

Answer

The term disaster can be defined as an incident which jeopardizes business operations and/or human life. It could be due to sabotage (human) or natural. Following is the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural plan is made when the system is normally working. After visualizing the disaster the action to be taken by different people of the organization are to be documented. This 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, is activated.
- Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning 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 the process for maintaining the plan.

- Awareness and education activities, which are designed to create an understanding of the disaster recovery process.
- 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.
- 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.
- Insurance papers and claim forms.
- Primary computer center 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 during the period of disruption such as manual preparation of invoices.
- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels, supplies and transport arrangements.

Question 4

Describe the methodology of developing a Business Continuity Plan.

(5 Marks, November 2008) & (4 Marks, May 2014)

Answer

The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The methodology emphasises 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 of availability to operations and key business functions;

(v) Focusing appropriately on disaster prevention and impact minimisation, 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 on-going business planning and system development processes in order that the plan remains viable over time.

The eight phases are given as follows:

(i) Pre-Planning Activities (Business Continuity Plan Initiation),

(ii) Vulnerability Assessment and General Definition of Requirements,

(iii) Business Impact Analysis,

(iv) Detailed Definition of Requirements,

(v) Plan Development,

(vi) Testing Program,

(vii) Maintenance Program, and

(viii) Initial Plan Testing and Plan Implementation.

Question 5

Briefly explain various types of system's back-up for the system and data together.

(5 Marks, November 2008)

Or

Write short note on Types of backups. ***(4 Marks, November 2014)***

Answer

Types of system's Back-ups: When the back-ups are taken of the system and data together, they are called Total System's Back-up. Various types of back-ups are given as follows:

- **Full Backup:** A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the

backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.

- **Incremental Backup:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

  Normally, incremental backup are very difficult to restore. One will have to start with recovering the last full backup, and then recovering files, which were charged subsequently from every subsequent incremental backup.

- **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 probably includes files that were already included in earlier differential backups.

- **Mirror back-up:** A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

Question 6

A company has decided to outsource its recovery process to a third party site. What are the issues that should be considered by the security administrators while drafting the contract?

(5 Marks, May 2010)

Answer

If a third-party site is to be used for 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;

- Procedures to ensure security of company's data from being accessed/damaged by other users of the facility; and
- What controls will be in place for working at the off-site facility.

Question 7

Discuss the various backup options considered by a security administrator when arranging alternate processing facility. ***(4 Marks, May 2011)***

Answer

Security administrators should consider the following backup options while arranging alternate processing facility:

- **Cold site:** If an organization can tolerate some down time, cold site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system, raised floors, air conditioning, power, communication lines, and so on. An organization can establish its own cold site facility or enter into an agreement with another organization to provide a cold site facility.
- **Hot site:** If fast recovery is critical, an organization might need hot site backup. All hardware and operations facilities will be available at the host site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organizations that have hot site needs.
- **Warm site:** It provides an intermediate level of backup. It has all cold site facilities in addition with hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.
- **Reciprocal agreement:** Two or more organizations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

Question 8

What are the elements to be included in the methodology for the development of disaster recovery / business resumption plan? ***(6 Marks, November 2012)***

OR

How an auditor will determine whether the disaster recovery plan was developed using a sound and robust methodology? Explain. ***(6 Marks, November 2013)***

Answer

The elements to be included in the methodology for the development of a disaster recovery/business resumption plan are given as follows:

- Identification and prioritization of the activities, which are essential for continuous functioning.
- Determining that the plan is based upon a business impact analysis, which considers the impact of the loss of essential functions.
- Determining that Operation managers and key employees participated in the development of the plan.
- Determining that the plan identifies the resources that will likely to be needed for recovery and the location of their availability.
- Determining that the plan is simple and easily understood so that it will be effective when it is needed.
- Determining that the plan is realistic in its assumptions.

Question 9

What are the goals of Business Continuity Plan? ***(4 Marks, November 2012)***

OR

Write a short note on 'goals of the business continuity plan'. ***(4 Marks, November 2013)***

Answer

The goals of a Business Continuity Plan should be to:

- identify the 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 efforts.

Question 10

While auditing a Disaster Recovery Plan (DRP) for information technology (IT) assets, what concerns are required to be addressed? Briefly explain. ***(4 Marks, May 2014)***

Answer

While auditing a Disaster Recovery Plan (DRP) for IT assets, the following concerns are required to be addressed:

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritization of critical applications and systems.
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.
- Does the disaster recovery/ business resumption plan include arrangements for emergency telecommunications?

- Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?
- Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weaknesses identified in the last tests were corrected.
- Determine if information backup procedures are sufficient to allow for recovery of critical data.
- Determine if copies of the plan are safeguarded by off-site storage.
- Does the disaster recovery/ business resumption plan include provisions for Personnel?

Question 11

While doing audit or self assessment of the BCM Program of an enterprise, briefly describe the matters to be verified. ***(6 Marks, November 2014)***

Answer

An audit or self-assessment of the enterprise's BCM (Business Continuity Management) program should verify that:

- All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
- The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements;
- The enterprise' BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;
- The enterprise's BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise;
- The enterprise's BCM maintenance and exercising programs have been effectively implemented;
- BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
- The enterprise has an ongoing program for BCM training and awareness;
- BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and
- Change control processes are in place and operate effectively.

Question 12

Explain the objectives of Business Continuity Management Policy briefly.

(4 Marks, November 2014)

Answer

The objective of Business Continuity Management Policy is to provide a structure through which:

- The loss to enterprise's business in terms of revenue loss, loss of reputation, loss of productivity and customer satisfaction is minimized.
- Critical services and activities undertaken by the enterprise operation for the customer will be identified.
- Plans will be developed to ensure continuity of key service delivery following a business
- Disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
- Invocation of incident management and business continuity plans can be managed.
- Incident Management Plans & Business Continuity Plans are subject to ongoing testing, revision and updation as required.
- Planning and management responsibility are assigned to a member of the relevant senior management team.

5

Acquisition, Development and Implementation of Information Systems

Question 1

Bring out the reasons as to why organizations fail to achieve their Systems Development Objectives? ***(12 Marks, November 2003)***

Answer

Following are the major reasons due to which organizations fail to achieve their system development objectives:

(i) **User Related Issues:** It refers to those issues where user/customer is reckoned as the primary agent. Some of the aspects with regard to this problem are mentioned as follows:

- **Shifting User Needs:** User requirements for IT are constantly changing. As these changes accelerate, there will be more requests for Information 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 purpose might change after the development process began.
- **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:** Often users do not participate in the development stage because they are preoccupied with their existing work, or do not understand the benefits of the new system. User apathy 'I have nothing to gain if I participate' is also a reason.
- **Inadequate Testing and User Training:** Often systems are not tested due to lack of time and rush to introduce the new system or because problems were not envisaged at the development stage. Inadequate user training may be a result of poor project planning, or lack of training techniques, or because user management does not release personnel for training due to operational pressure.

(ii) **Developer Related Issues:** It refers to the issues and challenges with regard to developers. Some of the critical bottlenecks are mentioned as follows:

- **Lack of Standard Project Management and System 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, system developers lack sufficient educational background and requisite state of the art skills. Furthermore, many companies do little to help their development personnel stay technically sound, and often a training plan and training budget do not exist.

(iii) **Management Related Issues:** It refers to the bottlenecks with regard to organizational set up, administrative and overall management to accomplish the system development goals. Some of such bottlenecks are mentioned as follows:

- **Lack of Senior Management Support and Involvement:** 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 may not allocate adequate resources, as well as budgetary control over use of resources, assigned to the project.
- **Development of Strategic Systems:** Because strategic decision making is unstructured, the requirements, specifications, and objectives for such development projects are difficult to define.

(iv) **New Technologies:** When an organization tries to create a competitive advantage by applying advance technologies, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the technology.

In order to overcome these aforementioned issues, organizations must execute a well-planned systems development process efficiently and effectively. Accordingly, a sound system development team is inevitable for project success.

Question 2

Explain the different conversion strategies used for conversion from a manual to a computerized system. ***(5 Marks, November 2003)***

OR

Describe various strategies for change over from manual system to computerised system.

(5 Marks, May 2006)

Answer

Different changeover strategies used for conversion from old system to new system are given

as follows:

- **Direct Implementation / Abrupt Change-Over:** This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. Fig 5.1 (i) depicts Direct Implementation, which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.

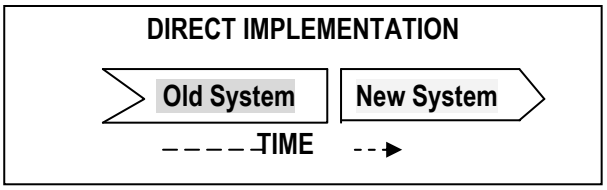

Fig. 5.1 (i): Direct Changeover

- **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually. For example, some new files may be converted and used by employees whilst other files continue to be used on the old system i.e. the new is brought in stages (phases). If a phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one as shown in Fig. 5.1(ii).

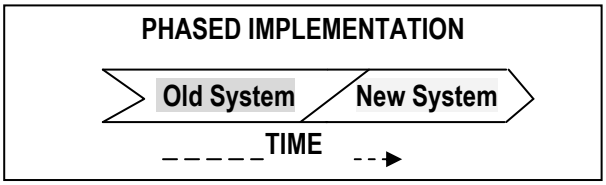

Fig. 5.1 (ii): Phased Changeover

- **Pilot Changeover:** With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with least disruption. For example - it might be tried out in one branch of the company or in one location. If successful the pilot is extended until it eventually replaces the old system completely. Fig. 5.1 (iii) depicts Pilot Implementation.

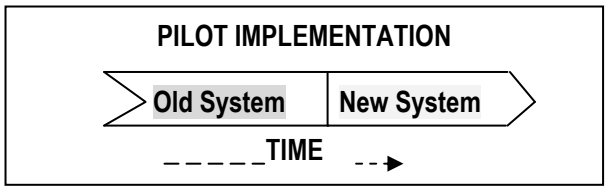

Fig. 5.1 (iii): Pilot Changeover

- **Parallel Changeover:** This is considered as a secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new systems come online. With this strategy, the old and the new system are both used alongside each other, both being able to operate independently. If all goes well, the old system is stopped and new system carries on as the only system. Fig. 5.1(iv) shows parallel implementation.

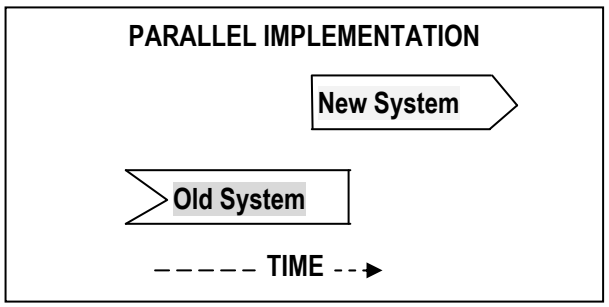

Fig. 5.1 (iv): Parallel Changeover

Question 3

Discuss briefly the advantages and disadvantages of any one conversion strategy.

(3 Marks, November 2003)

Answer

Advantages and disadvantages of most popular conversion strategy viz. Parallel conversion are discussed below:

Advantages: The advantage of running both systems in parallel includes the possibility of checking new data against old data in order to catch any errors in processing in the new system. Parallel processing also offers a feeling of security to users, who are not forced to make an abrupt change to the new system.

Disadvantages: It involves high cost of running two systems at the same time, and the burden on employees of virtually doubling their workload during conversion. Another disadvantage is that unless the system being replaced is a manual one, it is difficult to make comparisons between output of the new system and the old one. Supposedly, the new system was created to improve on the old one. Therefore, outputs from the systems should differ. Finally, it is understandable that employees who are faced with a choice between two systems will continue using the old one because of their familiarity with it.

Question 4

(a) What is a system development Life-cycle?

(b) Discuss the four steps of the prototyping approach in system development.

(2 + 8 Marks, May 2004)

Answer

(a) **System Development Life cycle** or SDLC is the set of activities that a system analyst has to carry out to develop and implement an information system under various approaches of development. It consists of mainly six activities: preliminary investigation, requirement analysis, design of system, development of software, system testing, implementation and maintenance. In most business situations, these activities are all closely related usually in- separable and even the order of the steps in these activities may be difficult to determine.

(b) Prototyping approach in system development can be viewed as a series of following four steps:

Step 1: Identify Information System Requirements: In traditional approach, the system requirements have to be identified before the development process starts. However, under prototype approach, the design team needs only fundamental system requirements to build the initial prototype, the process of determining them can be less formal and time-consuming than when performing traditional systems analysis. The team can develop the detailed requirements of the system later after users have had time to interact with the prototype and provide feedback.

Step 2: Develop the Initial Prototype: In this step, the designers create an initial base model – for example, using fourth-generation programming languages or CASE tools. In this phase, the goals are "rapid development" and "low cost." Thus, the designers give little or no consideration to internal controls, but instead emphasize on such system characteristics as "simplicity," "flexibility," and "ease of use." These characteristics enable users to interact with tentative versions of data entry display screens, menus, input prompts, and source documents. The users also need to be able to respond to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.

Step 3: Test and Revise: After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment. At the outset, users must be told that the prototype is incomplete and requires subsequent modifications based on their feedback. Thus, the designers ask users to record their likes and dislikes about the system and recommend changes. Using this feedback, the design team modifies the prototype as necessary and then resubmits the revised model to system users for revaluation. Thus, iterative process of modification and revaluation continues until the users are satisfied – commonly, through four to six interactions.

Step 4: Obtain User Signoff of the Approved Prototype: At the end of Step 3, users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not, do or provide. Approximately half of these approved prototypes become fully functional systems. The remaining, throwaway prototypes are not developed – typically because the modifications required to make them functional are too costly or in other ways not

practical. But this does not mean that the prototyping exercise has been a failure. To the contrary, it signals an impractical system and thus saves an organization a great deal of time and money.

Question 5

"The final step of the system implementation is its evaluation." What functions are being served by the system evaluation? Discuss development, operation and information evaluations. ***(10 Marks, November 2004)***

OR

What is the purpose of the system evaluation? How is it performed?

(5 Marks, May 2008)

Answer

Evaluation of the new system: The final step of the system implementation is evaluation. Evaluation provides the feedback necessary to assess the value of information and the performance of personnel and technology included in the newly designed system. This feedback serves two functions:

1. It provides information as to what adjustments to the information system may be necessary.
2. It provides information as to what adjustments should be made in approaching future information system development projects.

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

Development evaluation: Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. This is a rather straightforward evaluation. It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained. It may be noted that very few information systems have been developed on schedule and within budget. In fact, many information systems are developed without clearly defined schedules or budgets. Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.

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

1. Are all transactions processed on time?
2. Are all values computed accurately?

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

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

Information evaluation: An information system should also be evaluated in terms of information it provides. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operation evaluations. The objective of an information system is to provide information to support the organizational decision system. Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system. However, it is practically impossible to directly evaluate an information system's support for decision-making in an organization. It must be measured indirectly. User satisfaction can be used as a measure to evaluate the information provided by an information system. Measurement of user satisfaction can be accomplished using the interview and questionnaire technique. If management is generally satisfied with an information system, it is assumed that the system is meeting the requirements of the organization. If management is not satisfied, modifications ranging from minor adjustments to complete redesign may be required.

Question 6

Write short notes on the following:

(a) System Development Life-cycle. ***(5 Marks, November 2004)***

(b) Data Dictionary ***(5 Marks, May 2005, May 2007, May 2010)*** ***(4 Marks, May 2012)***

(c) System Maintenance ***(5 Marks, November 2005, May 2007, November 2008)*** ***(4 Marks, November 2011)***

(d) White Box Testing ***(5 Marks, June, 2009)***

(e) Black Box Testing ***(5 Marks, November 2009)***

(f) Regression Testing ***(4 Marks, November 2010)***

(g) Types of System Testing ***(4 Marks, November 2013)***

Answer

(a) System Development Life Cycle: The process of system development starts when management realizes that a particular business needs improvement. The system development life cycle method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system.

The system development life cycle method consists of the following activities:

(i) Preliminary investigation: It is undertaken when users come across a problem or opportunity and submit a formal request for a new system to the MIS department. This activity consists of three parts; request clarification, feasibility study and request approval.

(ii) Requirements analysis or systems analysis: In this stage, the analysts work closely with employees and managers of the organization for determining the information requirements of the users. Several fact-finding techniques and tools such as questionnaires, interviews, observing decision-maker behaviour and office environment, etc. are used for understanding the requirements of the users. As details are gathered, the analysts study the present system to identify its problems and shortcomings and identify the features which the new system should include to satisfy the new or changed user application environment.

(iii) Design of the system: It produces the details that state how a system will meet the requirements identified in the previous step. The analyst designs various reports/outputs, data entry procedures, inputs, files and database. He also selects file structures and data storage devices. These detailed design specifications are then passed on to the programming staff for software development.

(iv) Acquisition and development of software: In this stage, resource requirements such as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software developers may modify and then install purchased software or they may write new custom designed programs.

(v) System testing: Before the information system can be used, it must be tested. Special test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.

(vi) Implementation and maintenance: After system is found to be fit, it is implemented with actual data. After implementation, the system is maintained; it is modified to adapt to changing users and business needs.

(b) Data Dictionary – A data dictionary is a computer file that contains descriptive information about the data items in the files of an information system. Thus, it is a

computer file about data. Each computer record of a data dictionary contains information about a single data item used in the system. This information may include:

(i) Codes describing the data item's length, data type and range.

(ii) Identification of the source documents used to create the data item.

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

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

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

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

A data dictionary has a variety of uses as stated below:

- Programmers and system analysts can use it as a documentation aid.
- It can help accountants and auditors to establish an audit trail.
- It can be used to plan the flow of transaction data through the system.

It can serve as an important aid to document internal control procedures.

(c) System Maintenance: Most information systems require at least some modification after development. The need for modification arises from a failure to anticipate all requirements during system design and/or from changing organizational requirements. The changing organizational requirements continue to impact most information systems as long as they are in operation. Consequently periodic systems maintenance is required for most of the information systems. Systems maintenance involves adding new data elements, modifying reports, adding new report, changing calculation etc.

Maintenance can be categorized in the following two ways:

(i) Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.

(ii) Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.

(d) White Box Testing: It uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to select paths through the code and determines the appropriate outputs. It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit. While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the

product conforms to specifications and all the internal components are adequately exercised.

(e) Black Box Testing: Black Box Testing takes an external perspective of the test object, to derive test cases. These tests can be functional or non-functional, though usually functional. The test engineer has no prior knowledge of the test object's internal structure. The test designer selects typical inputs including simple, extreme, valid and invalid input-cases and executes to obtain assurance or uncover errors.

This method of test design is applicable to all levels of software testing i.e. unit, integration, functional testing, system and acceptance. The higher the level, the box is bigger and more complex, and the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested. If a module performs a function, which it is not supposed to, the black box test may not identify it.

(f) Usage of Regression Testing:

(i) All aspects of system remain functional after testing.

(ii) Change in one segment does not change the functionality of other segment.

Objectives:

(i) System documents remain current.

(ii) System test data and test conditions remain current.

(iii) Previously tested system functions properly without getting effected though changes are made in some other segment of application system.

How to Use:

- Test cases, which were used previously for the already tested segment is, re-run to ensure that the results of the segment tested currently and the results of same segment tested earlier, are same.
- Test automation is needed to carry out the test transactions (test condition execution) else the process is very time consuming and tedious.
- In this case of testing, cost/benefit should be carefully evaluated else the efforts spend on testing would be more and payback would be minimum.

(g) Types of System Testing: System testing is a process in which software and other system elements are tested as a whole. Major types of system testing that might be carried out, are given 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, availability, authentication, authorization 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:** 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.

Question 7

Explain different activities involved in conversion from manual system to computerized system.

(5 Marks, May 2005)

OR

Explain briefly various activities that should be completed for successful conversion of an existing system to the new information system. ***(10 Marks, November 2007)***

OR

What activities are involved in system conversion ? Explain them briefly.

(6 Marks, May 2013)

Answer

Activities involved in conversion: Conversion includes all those activities which must be completed to successfully convert from the existing manual system to the computerized information system. Fundamentally these activities can be classified as follows:

- Procedure conversion;
- File conversion;
- System conversion;
- Scheduling personnel and equipment; and
- Alternative plans in case of equipment failure.

These are briefly discussed as follows:

- **Procedure conversion:** Operating procedures should be completely documented for the

new system. This 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, outputs, 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. Brief meetings must be held when changes are taking place in order to inform all operating employees of any changes initiated. Revisions to operating procedures should be issued as quickly as possible. These efforts enhance the chances of successful conversion.

Once the new system is completely operational, the system implementation group should spend several days checking with all supervisory personnel about their respective areas.

- **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 data base) or off–line files. Present manual files are likely to be inaccurate and incomplete where deviations from the accepted formats are common. Computer generated files tend to be more accurate and consistent.

  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 the required output of the conversion program. The existing computer files should be kept for a period of time until the new system perform in stable manner. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.

- **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. A cut–off point is established so that data base and other data requirements can be updated to the cutoff point. 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. All differences must be reconciled. If necessary, appropriate changes are made to the new system and its computer programs. The old system can be dropped as soon as the data processing group is satisfied with the new system's performance.

- **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, however, the job becomes more routine.

  Before the new design project is complete, it is often necessary to schedule the new equipment. Some programs will be operational while others will be in various stages of

compiling and testing. Since production runs tend to push aside new program testing, the system manager must assign ample time for all individuals involved. Schedules should be set up by the system manager in co-ordination with departmental managers of operational units serviced by the equipment.

Just as the equipment must be scheduled for its maximum utilization, so must be personnel who operate the equipment. It is also imperative that personnel who enter input data and handle output data be included in the data processing schedule. Otherwise, data will not be available when the equipment needs it for processing.

- **Alternative plans in case of equipment failure:** Alternative-processing plans must be implemented in case of equipment failure. Who or what caused the failure is not as important in case of equipment failure as the fact that the system is down. Priorities must be given to those jobs critical to an organization, such as billing, payroll, and inventory. Critical jobs can be performed manually until the equipment is set right.

  Documentation of alternative plans is the responsibility of the computer section and should be fully covered by the organization's systems and procedures manual. It should state explicitly what the critical jobs are, how they are to be handled in case of equipment failure, where compatible equipment is located, who will be responsible for each area during downtime and what deadlines must be met during the emergency. A written manual of procedures concerning what steps must be undertaken will help to overcome the unfavorable situation. Otherwise, panic will result in use of the least efficient methods when time is of the essence.

Question 8

Describe any five functional areas of a system which needs to be analysed by system analyst for detailed investigation of the present system. ***(5 Marks, May 2005)***

OR

A Company is offering a wide range of products and services to its customers. It relies heavily on its existing information system to provide up to date information. The company wishes to enhance its existing system. You being an information system auditor, suggest how the investigation of the present information system should be conducted so that it can be further improved upon. ***(10 Marks, May 2006)***

OR

Discuss in detail, how the investigation of present system is conducted by the system analyst. ***(10 Marks, May 2008)***

OR

Discus in brief the various functional areas to be studied by a system analyst for a detailed investigation of the present system. ***(8 Marks, May 2011)***

Answer

Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. Enough information should be assembled so that a qualified person can understand the present system without visiting any of the operating departments. Review of existing methods, procedures, data flow, outputs, files, inputs and internal controls should be intensive in order to fully understand the present system and its related problems.

The following areas may be studied in depth:

- **Review historical aspects:** A brief history of the organization is a logical starting point for the 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 can provide an excellent historical perspective. A historical review of the organization chart can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should identify what system changes have occurred in the past. These should include operations that have been successful or unsuccessful with computer equipment 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 data can be 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 analysts 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 online and off ‐line files which are maintained in the organization as these will reveal information about data that are not contained in any output. The related cost of retrieving and processing 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's 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 equipment including data interface, data links, modems, dial-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 carryover 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 control may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipment 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 control and other important items are reviewed and analyzed in a top down manner, the process must be properly documented. The logical flow of the present information system may be depicted with the help of system flow charts. The physical flow of the existing system may be shown by employing data flow diagrams. During the process of developing the data flow diagram, work on data dictionary for the new information system should be begun. The data elements needed in the new system will often be found in the present system. Hence, it is wise to start the development of the data dictionary as early as possible.

  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 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

Each of these must be investigated thoroughly.

Question 9

Discuss the desired characteristics of a good coding system. ***(5 Marks, May 2005)***

OR

What are the characteristics of a good coded program ? ***(6 Marks, November 2012)***

Answer

A good coded program should have the following characteristics:

- **Reliability:** It refers to the consistency with which a program operates over a period of time. However, poor setting of parameters and hard coding of some data could result in the failure of a program after some time.
- **Robustness:** It refers to the applications' strength to uphold its operations in adverse situations by taking into account all possible inputs and outputs of a program even 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.
- **Efficiency:** It refers to the performance per unit.
- **Usability:** It refers to a user-friendly interface and easy-to-understand internal/external documentation.
- **Maintainability:** It refers to the ease of maintenance of program even in the absence of the program developer and includes narrations in the source code.

Question 10

What are the fact finding techniques used by a system analyst ? ***(5 Marks, November 2005)***

OR

Briefly explain the various fact finding techniques which are used by the system analyst for determining the needs of an organization. ***(5 Marks, November 2007)***

Answer

Fact Finding Techniques: Various fact-finding techniques which are used by the system analyst for determining users' needs are discussed below:

(i) Documents: Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the applications associated with the current system etc. Documents are a very good source of information about user needs and the current system. They are easy to collect, convey a lot of information and provide

relatively objective data. The analyst should ensure that the documents which he is collecting are current, accurate and contain up-to-date information.

(ii) Questionnaires: Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.

(iii) Interviews: Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide systems developer with a complete picture of the problems and opportunities. Interviews also give analyst the opportunity to note user reaction first-hand and to probe for further information.

(iv) Observation: In prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototype of a new system, the system can be successfully developed. In traditional approach, the analyst should visit the user site to watch how the work was taking place. Such a surprise visit often helps the analyst in getting a clear picture of the user's environment and to determine why a request for a new system was submitted.

Question 11

Discuss various issues that should be considered while designing systems input.

(10 Marks, November 2005)

OR

Discuss various issues that should be considered while designing system input.

(5 Marks, May 2008)

Answer

Various issues that should be considered while designing systems input are briefly discussed below:

Input design consists of developing specifications and procedures for data preparation, developing steps which are necessary to put transactions data into a usable form for processing, and data-entry, i.e., the activity of putting the data into the computer for processing.

A starting point for the input design process is a review of the information compiled during the requirement analysis phase. The analyst must review facts related to the current system such as what data are entered, who enters them, where they are entered, and when they are entered. This review highlights basic problems and difficulties with the present system. An understanding of the present system's input directs attention to those areas needing improvement for more efficient data entry.

(i) **Content:** The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. This can be quite complicated because

the new system often means new information and new information often requires new sources of data. Sometimes, the data needed for a new system are not available within the organization. Hence, the system designer has to prepare new documents for collecting such information.

(ii) **Timeliness:** In data processing, it is very important that data is inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system. Timely input of data is very important in transaction processing systems.

(iii) **Media:** Another important input consideration includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives are available in the market such as workstations, magnetic disc, OCR, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.

(iv) **Format:** After the data contents and media requirements are determined, input formats are considered. While specifying the record formats, for instance, the type and length of each data field as well as any other special characteristics must be defined. Designing input formats often requires the assistance of a professional programmer or database administrator.

(v) **Input Volume:** Input volume refers to the amount of data that has to be entered in the computer system at any one time. In some decision-support systems and many real-time transaction processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy which involves thousands of records that are handled by a centralized data entry department using key-to-tape or key-to-disk systems.

Question 12

What is prototyping approaches to systems development? Describe its advantages and disadvantages also. ***(10 Marks, November 2007)***

Answer

Prototyping approaches: Prototyping technique is used to develop smaller systems such as decision support systems, management information systems and expert systems. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full scale and fully operational system. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is develop the real system.

Prototyping can be viewed as a series of four steps:

Step 1: Identify Information System Requirements: In traditional approach, the system requirements have to be identified before the development process start. However, under prototype, the process of determining them can be less formal and time-consuming than when performing traditional systems analysis.

Step 2: Develop the Initial Prototype: In this step, the designers create an initial base model-for example, using fourth-general programming languages or CASE tools. The main goal of this stage is 'rapid development' and 'low cost'.

Step 3: Test and Revise: After finishing the initial prototype, the designers first demonstrate the model to users for experiment. At the outset, users must be told that the prototype is incomplete and requires subsequent modifications based on their feedback. Thus, the designers ask users to record their likes and dislikes about the system and recommend changes. Using this feedback, the design team modifies the prototype as necessary and then resubmits the revised model to system user for reevaluation. Thus interactive process of modification and reevaluation continues until the users are satisfied-commonly, through four to six interactions.

Step 4: Obtain User Signoff of the Approved Prototype: At the end of Step 3, users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not do or provide.

Advantages of Prototyping

1. Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of the users' needs and requirements than does the traditional system development approach.
2. 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.
3. 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.

Disadvantages of Prototyping

1. 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.
2. 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 make this system difficult to maintain.

3. Prototyping may cause behavioral problems with system users. These problems include dissatisfaction by users if system developers are unable to meet all user demands for improvements as well as dissatisfaction and impatience by user when they have to go through too many interactions of the prototype.

Question 13

Discuss the various activities which are part of the system development life cycle.

(5 Marks, November 2007)

OR

State and briefly explain six stages of System Development Life Cycle (SDLC).

(10 Marks, November 2008)

Answer

System Development Life Cycle: The system development process is initiated when it is realized that a particular business process of the organization needs computerization or improvement. The system development life cycle is a set of six activities which are closely related. These activities after a certain stage can be done parallel to each other. For example the development can be started for some components (sub-systems) which are at the advanced stage of designing. The systems development life cycle method consists of the following activities:

- Preliminary investigation,
- Requirements analysis or systems analysis,
- Design of system,
- Development of software,
- Systems testing, and
- Implementation and maintenance.

The activities are briefly explained below:

- **Preliminary investigation:** When the user comes across a problem in the existing system or a totally new requirement for computerization, a formal request has to be submitted for system development. It consists of three parts; Request Classification Feasibility Study and Request Approval. Generally the request submitted is not stated clearly: hence requires detailed study. On receipt of request and identification of needs, the feasibility study is conducted which includes the aspects related to technical, economic and operational feasibility and is normally conducted by a third party depending upon the quantum and size of the requirements. Approval is sought from top

management to initiate the system development.

- **Requirements analysis or systems analysis:** Once the request of the system development is approved, the detailed requirement study is conducted in close interaction with the concerned employees and managers to understand the detailed functioning, short-comings, bottlenecks and to determine the features to be included in the system catering to the needs and requirements of users. This process is termed as "System Requirement Study (SRS)" or System analysis.
- **Design of the system:** This activity evolves the methodology and steps to be included in the system to meet identified needs and requirements of the system. The analyst designs the various procedures, report, inputs, files and database structures and prepares the comprehensive system design. These specifications are then passed on to the Development Team for program coding and testing.
- **Acquisition and development of software:** Once the system design details are resolved and SRS is accepted by the user, the hardware and software details along with services requirements are determined and procured choosing the best-fit options. Subsequently, choices are made regarding which products to buy or lease from which vendors. The choice depends on many factors such as time, cost and availability of programmers. In case of in-house development, the analyst works closely with the programmers. The analyst also works with users to develop documentation for software and various procedure manuals.
- **Systems testing:** Once all the programs comprising the system have been developed and tested, the system needs to be tested as a whole. System testing is conducted with various probable options and conditions to ensure that it does not fail in any condition. The system is expected to run as per the specifications made in the SRS and users' expectations. Live test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.
- **Implementation and maintenance:** By the time of accomplishment of the above activities, it is ensured that the requisite hardware and software are installed and the users are trained on the new system to carry out operations independently. For sometimes, hand-holding may be done by the system development team. The operations are monitored closely to ensure users' satisfaction. The system is maintained and modified to adapt to changing needs of users and business to ensure long-term acceptance of the system.

Question 14

Explain software testing and state its objectives. ***(5 Marks, November 2008)***

Answer

Testing is a process used to identify the correctness, completeness and quality of developed computer software. In other words, testing is nothing but CRITICISM or COMPARISON, i.e. comparing the actual value with expected one.

One definition of testing is "the process of questioning a product in order to evaluate it", where the "questions" are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. The word testing means the dynamic analysis of the product—putting the product through its paces. Testing helps in verifying and validating if the software is working as it is intended to be working.

Objectives of Software Testing include:

- Testing is a process of executing a program with the intent of finding an error.
- A good test case is one that has a high probability of finding a yet undiscovered error.
- A successful test is one that uncovers a yet undiscovered error.

The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defect, it can only show that software defects are present.

Question 15

The top management of company has decided to develop a computer information system for its operations. Is it essential to conduct the feasibility study of system before implementing it? If answer is yes, state the reasons. Also discuss three different angles through which feasibility study of the system is to be conducted. ***(10 Marks, June, 2009)***

Answer

Yes, it is essential to carry out the feasibility study of the project before its implementation. After possible solution options are identified, project feasibility-the likelihood that these systems will be useful for the organization-is determined. Feasibility study refers to a process of evaluating alternative systems through various angles so that the most feasible and desirable system can be selected for development. It is carried out by system analysts.

The Feasibility Study of the system is undertaken from three angles i.e. Technical, Economic and Operational. The proposed system is evaluated from a technical view point first and if technically feasible, its impact on the organization and staff is assessed. If a compatible technical and social system can be devised, it is then tested for economic feasibility.

Technical Feasibility: It is concerned with hardware and software. Essentially, the analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following:

- Does the necessary technology exist to do what is suggested (and can it be acquired)?

- Does the proposed equipment have the technical capacity to hold the data required to run the new system?
- Will the proposed system provide an adequate response to inquiries, regardless of the number or location of users?
- Can the system be expanded if developed?
- Are there technical guarantees of accuracy, reliability, ease of access, and data security?

Some of the technical issues to be considered are given in the following table:

Table: Technical Issues

Design Considerations	Design Alternatives
Communications Channel configuration	Point to point, multidrop, or line sharing
Communications Channel	Telephone lines, coaxial cable, fiber optics, microwave, or satellite
Communications network	Centralized, decentralized, distributed, or local area
Computer programs	Independent vendor or in-house
Data storage medium	Tape, floppy disk, hard disk, or hard copy
Data storage structure	Files or database
File organization and access	Direct access or sequential files
Input medium	Keying, OCR, MICR, POS, EDI, or voice recognition
Operations	In-house or outsourcing
Output frequency	Instantaneous, hourly, daily, weekly, or monthly
Output medium	CRT, hard copy, voice, or turn-around document
Output scheduling	Pre-determined times or on demand
Printed output	Pre-printed forms or system-generated forms
Processor	Micro, mini, or mainframe
Transaction processing	Batch or online
Update frequency	Instantaneous, hourly, daily, weekly, or monthly

Due to tremendous advancements in computer field, the technology is available for most business data processing systems but sometimes not within the constraints of the firm's resources or its implementation schedule. Therefore, tradeoffs are often necessary. A technically feasible system may not be economically feasible or may be so sophisticated that the firm's personnel cannot effectively operate it.

Economic Feasibility: It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented. This is the most difficult aspect of the study. The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following:

- The cost of conducting a full system investigation.
- The cost of hardware and software for the class of applications being considered.
- The benefits in the form of reduced costs or fewer costly errors.
- The cost if nothing changes (i.e. the proposed system is not developed).

The procedure employed is the traditional cost-benefit study.

Operational Feasibility: It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. The support or lack of support that the firm's employees are likely to give to the system is a critical aspect of feasibility. A system can be highly feasible in all respects except the operational and fails miserably because of human problems. Some of the questions, which may help in conducting the operational feasibility of a project, are stated below:

- Is there sufficient support for the system from management and from users? If the current system is well liked and used to the extent that persons will not be able to see reasons for a change, there may be resistance.
- Are current business methods acceptable to user? If they are not, users may welcome a change that will bring about a more operational and useful system.
- Have the users been involved in planning and development of the project? Early involvement reduces chances of resistance to the system and changes in general and increases the likelihood of successful projects.

Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will loss of control result in any area? Will accessibility of information be lost? Will individual performance be poorer after implementation than before? Will performance be affected in an undesirable way? Will the system slow performance in any area?

Question 16

While testing a software, how will you involve the people working in the system areas?

(5 Marks, June, 2009)

Answer

Following are the main testing techniques which involve the people working in the system areas:

(i) *White Box Testing:* White box testing is a test case design method that uses the control structure of the procedural design to derive test cases. Test cases can be derived to

- guarantee that all independent paths within a module have been exercised at least once,
- exercise all logical decisions on their true and false sides,
- execute all loops at their boundaries and within their operational bounds, and
- exercise internal data structures to ensure their validity

(ii) *Unit Testing:* In computer programming, a unit test is a method of testing the correctness of a particular module of source code. The idea is to write test cases for every non-trivial function or method in the module so that each test case is separate from the others if possible. This type of testing is mostly done by the developers.

(iii) *Requirements Testing:* These test conditions are generalized ones, which become test cases as the SDLC progresses until system is fully operational. The main usage of this testing technique is

- to ensure that system performs correctly
- to ensure that correctness can be sustained for a considerable period of time.
- system can be tested for correctness through all phases of SDLC but in case of reliability the programs should be in place to make system operational.

(iv) *Regression Testing:* Under this testing technique, test cases, which were used previously for the already tested segment, are re-run to ensure that the results of the segment tested currently and the results of same segment being tested earlier are same. Test automation is needed to carry out the test transactions (test condition execution) else the process is very time consuming and tedious. In this case of testing, cost/benefit should be carefully evaluated else the efforts spend on testing would be more and payback would be minimum. The major objectives are as follows:

- System documents remain current.
- System test data and test conditions remain current.
- Previously tested system functions properly without getting effected though changes are made in some other segment of application system.

(v) *Manual Support Testing:* It involves testing of all the functions performed by the people while preparing the data and using these data from automated system. The major objectives of this testing technique are to

- verify that manual support documents and procedures are correct,
- determine that manual support responsibility is correct,
- determine that manual support people are adequately trained,
- determine that manual support and automated segment are properly interfaced.

(vi) *Internal System Testing: This technique is used to* ensure interconnection between application functions correctly. The major objectives of the testing are to ensure that

- proper parameters and data are correctly passed between the applications,
- documentation for involved system is correct and accurate,
- proper timing and coordination of functions exists between the application systems.

Question 17

Discuss the benefits and limitations of unit testing. ***(5 Marks, May 2010)***

Answer

Unit Testing: Unit testing is a software verification and validation method in which a programmer tests if individual units of source code are fit for use. A unit is the smallest testable part of an application, which may be an individual program, function, procedure, etc. or may belong to a base/super class, abstract class or derived/child class.

Unit tests are typically written and run by software developers to ensure that code meets its design and behaves as intended. The goal of unit testing is to isolate each component of the program and show that they are correct. A unit test provides a strict, written contract that the piece of code must satisfy.

There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows:

- **Functional Tests:** Functional Tests check 'whether programs do, what they are supposed to do or not'. The test plan specifies operating conditions, input values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.
- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
- **Stress Tests:** 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. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. For example, during a sort operation, the available memory can be reduced to find out whether the program is able to handle the situation.
- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

Question 18

As a person in-charge of System Development Life Cycle, you are assigned a job of developing a model for a new system, which combines the features of a prototyping model and the waterfall model. Which will be the model of your choice and what are its strengths and weaknesses? ***(8 Marks, November 2010)***

Answer

As a person in-charge of system development life cycle, the spiral model will be the choice. The spiral model is a software development process, combining elements of both design and prototyping-in-stages, in an effort to combine/ advantages of top-down and bottom-up concepts. It is a system development method, which combines the features of the prototyping model and the waterfall model. The spiral model is intended for large, expensive and complicated projects. Its major distinctiveness is given as follows:

(i) The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.

(ii) A preliminary design is created for the new system. This phase is the most important part of 'Spiral Model' in which all possible alternatives that can help in developing a cost effective project are analyzed and strategies are decided to use them. This phase has been added specially in order to identify and resolve all the possible risks in the project development. If risks indicate any kind of uncertainty in requirements, prototyping may be used to proceed with the available data and find out possible solution in order to deal with the potential changes in the requirements.

(iii) A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.

(iv) A second prototype is evolved by a fourfold procedure:

- evaluating the first prototype in terms of its strengths, weaknesses, and risks;
- defining the requirements of the second prototype;
- planning and designing the second prototype; and
- constructing and testing the second prototype.

Game development is a main area where the spiral model is used and needed, that is because of the size and the constantly shifting goals of those large projects.

Strengths:

(i) Enhance risk avoidance;

(ii) Useful in helping to select the best methodology to follow for development of a given software iteration based on project risk.

(iii) Can incorporate waterfall, prototyping and incremental methodologies as special cases in the framework, and provide guidance as to which combinations of these models best fits a given software iteration, based upon the type of project risk.

Weaknesses:

(i) Challenges to determine the exact composition of development methodologies to use for each iteration around the spiral.

(ii) Highly customized to each project and thus is quite complex, limiting reusability.

(iii) A skilled and experienced project manager required to determine how to apply it to any given project.

(iv) No established controls for moving from one cycle to another cycle. Without controls, each cycle may generate, more work for the next cycle.

(v) No firm deadlines cycles continue with no clean termination condition, so there is an inherent risk of not meeting budget or schedule.

Question 19

From the perspective of IS audit, what are the advantages of System Development Life Cycle?

(4 Marks, November 2010)

Answer

From the perspective of the IS Audit, following are the possible advantages of SDLC:

- The IS auditor can have clear understanding of 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/her examination, can state in his/her report about the compliance by the IS management with the procedures, if any, set by management.
- If the IS Auditor has technical knowledge and ability to handle different areas of SDLC, s/he 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.

Question 20

At the end of analysis phase, the System Analyst prepares a document called "Systems Requirement Specifications (SRS)". Write the contents of SRS. ***(4 Marks, November 2011)***

Answer

At the end of the analysis phase, the System Analyst prepares a document called "Systems Requirement Specifications (SRS)". A SRS contains the following:

- **Introduction:** Goals and Objectives of the software context of the computer-based system;

- **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.

Question 21

Following are involved in the System Development Life Cycle (SDLC). Discuss their roles:

(i) Project Manager

(ii) System Analyst

(iii) Database Administrator (DBA)

(iv) IS Auditor ***(4 Marks, November 2011)***

Answer

(i) Project Manager: A project manager is normally responsible for more than one project and liaisons with the client or the affected functions. S/he is responsible for delivery of the project within the time and budget and periodically reviewing the progress of the project with the project leader and his/her team.

(ii) Systems Analyst: The systems/business analysts' main responsibility is to conduct interviews with users and understand their requirements. S/he is a link between the users and the programmers to convert the users requirements in the system requirements and plays a pivotal role in the Requirements analysis and Design phase.

(iii) Database Administrator (DBA): The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The DBA handles multiple projects; ensures the integrity and security of

information stored in the database and also helps the application development team in database performance issues. Inclusion of new data elements has to be done only with the approval of the database administrator.

(iv) IS Auditor: As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. He should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.

Question 22

What are the major activities involved in the design of a database? ***(4 Marks, May 2012)***

Or

Write short note on Design of database. ***(4 Marks, Nov. 2014)***

Answer

The designing of a database involves four major activities, which are given as follows:

- **Conceptual Modeling:** These describe the application domain via entities/objects, attributes of these entities/objects and static and dynamic constraints on these entities/objects, their attributes, and their relationships.
- **Data Modeling:** Conceptual Models need to be translated into data models so that they can be accessed and manipulated by both high-level and low-level programming languages.
- **Storage Structure Design:** Decisions must be made on how to linearize and partition the data structure so that it can be stored on some device. For example- tuples (row) in a relational data model must be assigned to records, and relationships among records might be established via symbolic pointer addresses.
- **Physical Layout Design:** Decisions must be made on how to distribute the storage structure across specific storage media and locations –for example, the cylinders, tracks, and sectors on a disk and the computers in a LAN or WAN.

Question 23

What is the goal of a prototype model approach of software development? Enumerate the strength of this model. ***(6 Marks, May 2013)***

Answer

The goal of a prototyping model is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full-scale and fully operational system.

As users work with the prototype, they make suggestions about the ways to improve it. These suggestions are then incorporated into another prototype, which is also used and evaluated and so on. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

Major strengths of Prototyping model are given as follows:

- Prototyping model improves both user participation in system development and communication among project stakeholders.
- This is 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.
- It has the potential for exploiting knowledge gained in an early iteration as later iterations are developed.
- This helps to easily identify confusing or difficult functions and missing functionality.
- This may generate specifications for a production application.
- This encourages innovation and flexible designs.
- The model 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 systems 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.

Question 24

Describe the Agile Methodology of system development. Describe its strength.

(6 Marks, November 2013)

Or

Define the Agile model of software development and discuss its strengths.

(6 Marks, November 2014)

Answer

Agile Methodology: This is a group of software development methodologies based on the *iterative and incremental* development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

It promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.

Major strengths of agile methodology are given as follows:

- Agile methodology has the concept of an adaptive team, which is able to respond to the changing requirements.
- The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirements of the customer have changed.
- Face-to-face communication and continuous inputs from customer representative leaves no space for guesswork.
- The documentation is crisp and to-the-point to save time.
- The end result is the high quality software in least possible time duration and satisfied customer.

Question 25

Describe the strength of waterfall approach to system development. ***(4 Marks, May 2014)***

Answer

Major strengths of waterfall approach are given as follows:

- This model is 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 help to ensure the quality, reliability, adequacy and maintainability of the developed software.
- Progress of system development is measurable in this model.
- It conserves resources also.

Question 26

Briefly explain about various categories of software maintenance used in System Development Life Cycle (SDLC). ***(6 Marks, May 2014)***

Answer

Various categories of software maintenance are given as follows:

- **Scheduled maintenance:** Scheduled maintenance is anticipated and can be planned; for example, implementation of a new inventory coding scheme can be planned in advance.
- **Rescue maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested, should have few occasions of rescue maintenance.
- **Corrective maintenance:** Corrective maintenance 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.
- **Adaptive maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The need for adaptive maintenance can only be recognized by monitoring the environment.
- **Perfective maintenance:** Perfective maintenance 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:** Preventive maintenance concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

6

Auditing of Information Systems

Question 1

(a) What is the sole purpose of an Information System (IS) Audit? ***(2 Marks)***

(b) What is the role of an IS Auditor? ***(2 Marks, November 2003)***

Answer

(a) The sole purpose of an Information system audit is to evaluate and review the adequacy of automated information systems to meet processing needs, to evaluate the adequacy of internal controls, and to ensure that assets controlled by those systems are adequately safeguarded.

(b) The Information System (IS) auditor is responsible for establishing control objectives that reduce or eliminate potential exposure to control risks. After the objectives of the audit have been established, the auditor must review the audit subject and evaluate the results of the review to find out areas that need some improvement. IS auditor should submit a report to the management, recommending actions that will provide a reasonable level of control over the assets of the entity.

Question 2

Write a short note on following:

(a) Integrated test facility ***(5 Marks, May 2004, November 2006)***

(b) Continuous and Intermittent Simulation (CIS) ***(4 Marks, May 2014)***

Answer

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

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

(b) Continuous and Intermittent Simulation (CIS): This is a variation of the System Control Audit Review File (SCARF) continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:

- The database management system reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
- CIS replicates or simulates the application system processing.
- Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.
- Exceptions identified by CIS are written to an exception log file.
- The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

Question 3

"In On-line systems, conventional audit trail is difficult and almost impossible." Why? Explain the kind of audit techniques used in such system. ***(10 Marks, November 2004)***

Answer

Historically, auditors have placed substantial reliance in evidence-collection work on the paper trail that documents the sequence of events that have occurred within an information system. Paper based audit trails have been progressively disappearing as online computer-based systems have replaced manual systems and as source documents have given a way to screen based inputs and outputs. In a batch processing system, one can still expect to find a visible trail of "run-to-run " controls, which can be reconciled to the original input batch totals. In such systems, it is unusual to find any significant loss of audit trails regarding the control totals. In online systems, however, data are stored in device-oriented rather than human-oriented form. Moreover, data files belonging to more than one application may be updated simultaneously by each individual transaction. In such systems, traditional run-to-run controls do not exist and the potential for loss of audit trail is significant.

In a batch processing systems, the test data is prepared by an auditor for audit purposes and the results are obtained from the program under execution and copy of relevant files. The results are compared with the predetermined correct outputs. Any discrepancies indicating processing errors or control deficiencies etc. are thoroughly investigated. In on-line systems, such kind of audit trail is not desirable since millions of transactions can be processed in a short time. In such cases, evidence gathered after data processing is insufficient for audit purposes. In addition, since many on-line systems process transactions continuously, it is difficult or impossible to stop the system in order to perform audit tests. Hence, the auditor needs to identify problems that can occur in an information system on a more timely basis. For this reason, a set of audit techniques has been developed to collect evidence at the same time as an application system undertakes processing of its production data.

Following are some of the audit techniques, which are being used for on-line systems :

(A) Concurrent Audit Techniques: These techniques can be used to continually monitor the system and collect audit evidence while live data are processed during regular operating hours. As the name suggests, this type of audit technique uses embedded audit modules, which are segments of program codes that perform audit functions. They also report test results to the auditors and store the evidence collected for the auditor's review. These techniques are often time consuming and difficult to use, but are less so, if incorporated when programs are developed.

There are five such techniques, which auditors commonly use. These are :

(i) Integrated Test Facility (ITF): In this technique, a small set of fictitious records is placed in the master file. Processing test transactions to update these dummy records will not affect the actual records. Actual and fictitious records are concurrently processed together, without the knowledge of employees. Auditor compares the output of dummy records with expected results and its controls to verify the correctness of the system.

(ii) Snapshot Technique: This technique examines the way transactions are processed. Selected transactions are marked with special code that triggers the snapshot processes. Audit modules in the program record these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed.

(iii) SCARF: System Control Audit Review File uses embedded audit modules to continuously monitor transaction activities and collect data on transactions with special audit significance. The data is recorded in a SCARF file, which may have been exceptional transactions. Periodically the auditor receives a print out of the SCARF file, examines the information to identify any questionable transactions, and performs any necessary follow up investigation.

(iv) **Audit Hooks:** These are audit routines that flag suspicious transactions. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach, known as "real-time notification", displays a message on the auditor's terminal.

(v) **CIS:** Continuous and intermittent simulation embeds an audit module in a DBMS. This module examines all transactions that update the DBMS using criterion similar to those of SCARF. If a transaction has special audit significance, the module independently processes the data, records the results and compares them with those obtained by the DBMS. Discrepancies are noted and details are investigated.

(B) Analysis of program logic: If a serious natured unauthorized code is found, the auditor goes for detailed analysis of the program logic. This is a difficult task and the auditor must be well versed with the programming language. These days following software packages serve as aids in this analysis.

- Automated flowcharting programs
- Automated decision table programs.
- Scanning Routine.
- Mapping Programs.
- Program tracing.

Question 4

Discuss various ways in which audit trail can be used to support security objectives.

(5 Marks, November 2005)

Answer

Audit trails can be used to support security objectives in the following three ways:

- **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.
- **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 existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in 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.

- **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. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

Question 5

What is the significance of input validation control? Describe briefly three different levels of input validation controls used in computerized information system. ***(10 Marks, May 2006)***

Answer

Input Validation Controls: These controls are intended to detect errors in transaction data before the data are processed. Validation procedures are most effective when they are performed as close to the source of the transactions as possible. However, depending on the type of Computer Based Information Systems (CBISs) in use, input validation may occur at various points in the system. For example, some validation procedures require making references against the current master file. Computer Based Information Systems (CBISs) using real-time processing or batch processing with direct access master files can validate data at the input stage. Some validation procedures are performed by each processing module prior to updating the master file record.

Three levels of input validation controls are given as follows:

- **Field Interrogation***:* It involves programmed procedures that examine the characters of the data in the field. The following are some common types of field interrogation. Various field checks used to ensure data integrity have been described below:
    - **Limit Check:** This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error exceeding certain pre-established limits has occurred.
    - **Picture Checks:** These check against entry of incorrect/invalid characters.
    - **Valid Code Checks:** Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in (direct access) files.
    - **Check Digit:** One method for detecting data coding errors is a check digit. A check digit is a control digit (or digits) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing. The check digit can be located anywhere in the code, as a prefix, a suffix, or embedded someplace in the middle.

- **Arithmetic Checks:** Simple Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.

  Example: The discounted amount for ₹ 4,000 at 5% discounted may be computed twice by the following different ways:

  4,000 – 4,000 × 5/100 = 3,800 or

  Next time again at

  (3800/(100-5))*100.

- **Cross Checks:** may be employed to verify fields appearing in different files to see that the result tally.

- **Record Interrogation***:* These are discussed as follows:
  - **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?
  - **Valid Sign:** The contents of one field may determine which sign is valid for a numeric field.
  - **Sequence Check:** If physical records follow a required order matching with logical records.

- **File Interrogation***:* These are discussed as follows:
  - **Version Usage:** Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file is processed.
  - **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for processing. Where there is a manual process for loading files, external labeling is important to ensure that the correct file is being processed. Where *there is an automated tape loader system, internal labeling is more important.*
  - **Data File Security:** Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability.
  - **Before and after Image and Logging:** The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.
  - **File Updating and Maintenance Authorization:** Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.

- **Parity Check:** When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.

Question 6

Describe the various security components available in a Secure Operating system.

(5 Marks, May 2006)

Answer

Operating System Security: Operating system security involves policy, procedures and controls that determine who can access the operating system, which resources they can access, and what actions they can take. The following security components are found in secure operating system:

(i) **Log-on Procedure:** A log-on procedure is the first line of defence against unauthorized access. When the user initiates the log-on process by entering user id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized. If password or ID is entered incorrectly, then after a specified number of attempts, the system should lock out the user from the system.

(ii) **Access token:** If the log on attempt is successful, the OS creates an access token that contains key information about the user including user ID, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session.

(iii) **Access control list:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her ID and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access.

(iv) **Discretionary Access Control:** The system administrator usually determines who is granted access to specific resources and maintains the access control list. However, in distributes system, resources may be controlled by the end-use. Resource owners in this setting may be granted discretionary access control, which allows them to grant access privileges to other users. For example, the controller who is owner of the general ledger grants read only privilege to the budgeting department while accounts payable manager is granted both read and write permission to the ledger.

Question 7

Discuss some common types of field interrogation as a validation control procedure in an EDP set up. ***(5 Marks, November 2006)***

Answer

Some common types of field interrogation as a validation control procedure in an EDP set up are discussed below:

(1) **Limit Checks:** The field is checked by the program to ensure that its value lies within certain predefined limits.

(2) **Picture checks:** These check against entry of incorrect characters into processing.

(3) **Valid Code Checks:** Checks are made against predetermined transactions codes, tables or other data to ensure that input data are valid. They may either be embedded in the programs or stored in files.

(4) **Check digit:** It is an extra digit that is added to the code when it is originally assigned. It allows the integrity of the code to be established during subsequent processing.

(5) **Arithmetic Checks:** Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.

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

Question 8

Describe major advantages of continuous audit techniques. ***(5 Marks, May 2010)***

Answer

Major advantages of continuous audit techniques are given as follows:

- **Timely, Comprehensive and Detailed Auditing –** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability –** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives –** Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users –** Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

Question 9

As an IS Auditor, explain the types of information collected for auditing by using System Control Audit Review File (SCARF) technique. ***(4 Marks, May 2011)***

OR

What do you mean by 'System Control Audit Review File' (SCARF)? What types of information can be collected by Auditor using SCARF? ***(6 Marks, May 2013)***

Answer

System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written on a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Auditors might use SCARF technique to collect the following types of information:

- **Application System Errors -** SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and Procedural Variances -** Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System Exception -** SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical Sample -** Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- **Snapshots and Extended Records -** Snapshots and extended records can be written into the SCARF file and printed when required.
- **Profiling Data -** Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance Measurement -** Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

Question 10

In what ways, an audit trails is used to support security objectives? Describe each one of them. ***(4 Marks, November 2011)***

Answer

Audit trails can be used to support security objectives in the following three ways:

- **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.
- **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 existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in 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.
- **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. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

Question 11

Describe the advantage and disadvantage of Continuous Auditing Techniques in brief.

(4 Marks, November 2011)

Or

Briefly describe the advantages and disadvantages of continuous auditing techniques.

(6 Marks, May 2014)

Answer

Continuous Auditing Technique: Continuous auditing enables auditors to shift their focus from the traditional 'transaction' audit to the 'system and operations' audit.

Advantages: Some of the advantages of continuous audit techniques are as under:

- **Timely, comprehensive and detailed auditing:** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.

- **Surprise test capability:** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives:** Continuous audit techniques provides information to systems staff regarding the testing to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users:** Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

Disadvantages: The following are some of the disadvantages and limitations of the continuous audit system:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

Question 12

What is the skill set expected from an IS Auditor? ***(6 Marks, May 2012)***

OR

As an IS Auditor, what are the steps to be followed by you while conducting IT auditing?

(6 Marks, November 2012)

Answer

Different audit organizations go about IS auditing in different ways and individual auditors have their own favourite ways of working. However, it can be categorized into the following major stages:

(i) **Scoping and pre-audit survey:** Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. Information sources at this stage include background reading and web

browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

(ii) **Planning and preparation:** During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

(iii) **Fieldwork:** Gathering evidence by interviewing staff and managers, reviewing documents, and observing processes etc.

(iv) **Analysis:** This step involves desperately sorting out, reviewing and trying to make sense of all the evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

(v) **Reporting:** Reporting to the management is done after analysis of evidence gathered and analysed.

(vi) **Closure:** Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

Question 13

Explain the set of skills that is generally expected of an IS auditor. ***(6 Marks, November 2012)***

Answer

The set of skills that is generally expected of an IS auditor includes:

- 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 procedural 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.

Question 14

What is the scope of IS Audit process? Explain the categories of IS Audit.

(6 Marks, November 2012)

Answer

The scope of IS Audit process should include the examination and evaluation of the adequacy and effectiveness of the system of internal controls and the quality of performance by the information system. In addition, IS Audit process will also examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists so that

objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The scope of the audit will also include the internal control system/s for the use and protection of information and the information systems, such as, *Data, Application systems, Technology, Facilities, and People.*

IS Audit has been categorized into the following five major types:

- **Systems and Applications:** An audit to verify that systems and applications are appropriate, efficient, and 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, accurately, and efficiently 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 servers.

Question 15

What is scope of output control of an application system ? Suggest various types of output controls which are enforced for confidentiality, integrity and consistency of output.

(6 Marks, May 2013)

Answer

The scope of Output controls of an application system is given as follows:

To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.

Various types of output controls, which are enforced for confidentiality, integrity and consistency of output, are given as follows:

- **Storage and logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments etc.
- **Logging of output program executions:** When programs used for output of data are

executed, it should be logged and monitored. In the absence of control over such output program executions, confidentiality of data could be compromised.

- **Spooling/Queuing:** This is a process used to ensure that the user is able to continue working, even before the print operation is completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is them "spooled" to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents waiting to be printed on a particular printer. This queue should not be subject to unauthorized modifications.
- **Controls over printing:** It should be ensured that unauthorized disclosure of information printed is prevented. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
- **Report distribution and collection controls:** Distribution of reports should be made in a secure way to ensure unauthorized disclosure of data. A log should be maintained as to what reports were generated and to whom it was distributed. Where users have to collect reports; the user should be responsible for timely collection of the report especially if it is printed in a public area. A log should be maintained as to what reports where printed and which of them where collected. Uncollected reports should be stored securely.
- **Retention controls:** Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced.
- **Existence/Recovery Controls:** These are needed to recover output in the event that it is lost or destroyed. If the output is written to a spool of files or report files and has been kept, then recovering and new generation is easy and straight-forward.

Question 16

'Real time information system needs real time audit techniques like Integrated Test Facility (ITF) to provide continuous assurance.' Define and explain the ITF methodology.

(6 Marks, November 2013)

Answer

Integrated Test Facility (ITF): ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases, the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.

Detailed explanation of ITF technique is given as follows:

Methods of Entering Test Data: The transactions to be tested have to be tagged. The application system has to be programmed to recognize the tagged transactions and have them invoked two updates, one to the application system master file record and one to the ITF dummy entity. Auditors can also embed audit software modules in the application system programs to recognize transactions having certain characteristics as ITF transactions. Tagging live transactions as ITF transactions has the advantages of ease of use and testing with transactions representative of normal system processing. However, use of live data could mean that the limiting conditions within the system are not tested and embedded modules may interfere with the production processing.

The auditors may also use test data that is specially prepared. Test transactions would be entered along with the production input into the application system. In this approach, the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way. However, preparation of the test data could be time consuming and costly.

Methods of Removing the Effects of ITF Transactions: The presence of ITF transactions within an application system affects the output results obtained. The effects of these transactions have to be removed. The application system may be programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users. Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions. Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal in which the effects of the transactions are not really removed.

Question 17

As an IS auditor, what are the risks reviewed by you relating to IT systems and processes as part of your functions? ***(4 Marks, November 2014)***

Answer

IS (Information Systems) Auditors review risks relating to IT systems and processes; some of them are as follows:

- Inadequate information security controls (e.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.)
- Inefficient use of 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 a lack of policy for use of
- Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.).
- IT-related frauds (including phishing, hacking etc).

Question 18

Compared to traditional audit, evidence collection has become more challenging with the use of computers to the auditors. What are the issues which affect evidence collection and understanding the reliability of controls in financial audit? ***(6 Marks, November 2014)***

Answer

The issues which affect evidence collection and understanding the reliability of controls in financial audit are as follows:

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system.
- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of EDI will result in less paperwork being available for audit examination.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Lack of availability of output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
- **Audit evidence:** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalized) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
- **Legal issues:** The use of computers to carry out trading activities is also increasing. More organizations in both the public and private sector intend to make use of EDI and electronic trading over the internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and the parties to the contract.

7

Information Technology Regulatory Issues

Question 1

Define the following important terms in the light of the Section 2 of the I.T. Act, 2000:

(i) Affixing digital signature

(ii) Asymmetric crypto system

(iii) Computer network

(iv) Private and Public keys

(v) Secure system ***(10 Marks, November 2004)***

Answer

The definition of important terms according to Section 2 of the Information Technology Act, 2000 is as under:

(i) **"Affixing digital signature"** with its grammatical variation and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

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

(iii) **"Computer network"** means the interconnection of one or more computers through –

(a) the use of satellite, microwave, terrestrial line or other communication media; and

(b) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

(iv) **"Private and public keys"** refer to a key pair used in an asymmetric crypto system. Private key means the key used to create a digital signature whereas public key is used to verify the same and is listed in the Digital Signature Certificate.

(v) **"Secure system"** means computer hardware, software and procedures that

- are reasonably secure from unauthorized access and misuse;
- provide a reasonable level of reliability and correct operation;

- are reasonably suited to performing the intended functions; and
- adhere to generally accepted security procedures.

Question 2

Explain the objectives and scope of the Information Technology Act 2000.

(5 Marks, May 2005, November 2007 & 4 Marks, May 2012)

Answer

Major objectives of the Information Technology Act 2000 are given as follows:

- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
- To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
- To facilitate electronic filing of documents with Government departments;
- To facilitate electronic storage of data;
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- To give legal recognition for keeping of books of accounts by banker's in electronic form; and
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

Scope of the Act: This Act is applicable to whole of India, unless otherwise provided in the Act. It also applies to any offence or contravention there under committed outside India by any person.

Different provisions of this Act came into force on the different dates as notified by the Central Government.

The Act shall not be applicable to the following:

- a negotiable instrument as defined in Section 13 of the Negotiable Instruments Act, 1881;
- a Power of Attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882;
- a trust as defined in Section 3 of the Indian Trusts Act, 1882;
- a will as defined in Section (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
- any contract for the sale or conveyance of immovable property or any interest in such property;

Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Question 3

State the liabilities of companies under section 85 of Information Technology Act, 2000.

(5 Marks, November 2008)

Answer

Liability of Companies under Section 85 of Information Technology Act, 2000: Where a company commits any offence under this Act or any rule thereunder, every person who, at the time of the contravention, was in charge of and was responsible for the conduct of the business of the company shall be guilty of the contravention. However, he shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention.

Further, where a contravention has been committed by a company, and it is proved that the contravention took place with the connivance or consent of or due to any negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty and shall be liable to be proceeded against and punished accordingly.

For the purposes of this section, 'company' includes a firm or other association of persons and 'director' in relation to a firm means a partner in the firm.

The Information Technology Act will go a long way in facilitating and regulating electronic commerce. It has provided a legal framework for smooth conduct of e-commerce. It has tackled the following legal issues associated with e-commerce:

- Requirement of writing
- Requirement of a document
- Requirement of a signature and
- Requirement of legal recognition for electronic messages,
- Records and documents to be admitted in evidence in a court of law.

Question 4

What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature? ***(5 Marks, June 2009)***

OR

How does the Information Technology Act 2000 enable the authentication of records using digital signatures? ***(5 Marks, November 2009)***

OR

Write short notes on *Authentication of electronic records in Information Technology (Amended) Act 2008.* ***(4 Marks, May 2011)***

Answer

Chapter-II of IT Act, 2000 gives legal recognition to electronic records and digital signatures. It contains only section 3.

[Section 3] **Authentication of Electronic Records:**

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Question 5

How does the Information Technology Act, 2000 enable the objective of the Government in spreading e-governance? ***(5 Marks, November 2009)***

Answer

Chapter III is one of the most important chapters of IT Act 2000. It deals with the procedures to be followed for sending and receiving of electronic records. This chapter contains sections 4 to 10.

Section 4 - This section provides for *legal recognition of electronic records.*

Section 5 - This section provides for *legal recognition of Digital Signatures.*

Section 6 - lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue

or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

Section 7 - This section provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained in the electronic form with the following conditions:

(i) the information therein remains accessible so as to be usable subsequently,

(ii) it is retained in its original format ,

(iii) the details such as origin, destination, dates and time of dispatch or receipt of such electronic record.

Section 8 - It provides for the publication of rules, regulations and notifications in the Electronic Gazette.

Question 6

Define the following terms related to Information Technology Act, 2000:

(i) Computer contaminant

(ii) Cyber cafe

(iii) Electronic form

(iv) Traffic data

(v) Asymmetric crypto system. ***(5 Marks, May 2010)***

Answer

(i) Computer Contaminant: It refers to any set of computer instructions that are designed:

- to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or
- by any means to disrupt the normal operation of the computer, computer system, or computer network.

(ii) Cyber Cafe: It refers to any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.

(iii) Electronic Form: It refers to any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

(iv) Traffic Data: It refers to any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data size, duration or type of underlying service or any other information.

(v) **Asymmetric crypto system:** It refers to a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Question 7

Describe the 'Power to make rules by Central Government in respect of Electronic Signature' in the light of Section 10 of Information Technology Act 2000. ***(4 Marks, May 2012)***

Answer

Section 10 gives the Central Government following powers to make rules in respect of Electronic Signature

(a) specify the type of Electronic Signature;

(b) specify how Electronic Signature shall be affixed and the format of the signatures;

(c) to identify the person who has affixed the Electronic Signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to Electronic Signature.

Question 8

How is the term 'Electronic Record' defined in IT (Amended) Act 2008? What is the provision given in the IT Act for the retention of Electronic Records? ***(6 Marks, May 2012)***

Answer

"Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

[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.

Question 9

Mr. A has received some information about Mr. B on his cellphone. He knows that this information has been stolen by the sender. He not only retained this information but also sends it to Mr. B and his friends. Because of this act Mr. B is annoyed and his life is in danger.

Mr. B seeks your advice, under what sections of Information Technology (Amendment) Act, 2008, he can file an FIR with police? Advise Mr. B detailing the applicable sections of the Act.

(6 Marks, May 2013)

Answer

It is not clear whether Mr. B wants to file an FIR with police against Mr. A or sender, who has stolen his information or both.

Considering the most feasible assumption that if Mr. B wants to file an FIR against Mr. A then he may file the same under the following Section of Information Technology (Amendment) Act, 2008:

- Section 66 A: Punishment for sending offensive messages through communication service, etc.;
- Section 66 B: Punishment for dishonestly receiving stolen computer resource or communication device; and
- Section 66 E: Punishment for violation of privacy.

All these applicable sections in this case are given as follows:

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

[Section 66 B] Punishment for dishonestly receiving stolen computer resource or communication device.

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

[Section 66E] Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

However, the answer may also be written considering the other two assumptions, accordingly.

Question 10

Mr. A is regularly sending obscene in electronic form to Ms. B. When Ms. B made a complaint to Police, it was found that all the communications were sent through XYZ network service provider. Police have held both Mr. A and XYZ network service provider as liable for this act. Suggest under what provisions of Information Technology (Amendment) Act, 2008, the XYZ network service provider can get exemption from the liability? Also discuss the relevant provisions of the above section. ***(4 Marks, May 2014)***

Answer

As per Information Technology (Amendment) Act 2008, the XYZ network service provider can get exemption from the liability under provisions of sub-sections 1 and 2 of **Section 79: Exemption from liability of intermediary in certain cases**.

The relevant provisions of the above section are given as follows:

[Section 79] Exemption from liability of intermediary in certain cases:

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

Question 11

Discuss briefly, the four phases of Information Security Management System (ISMS) prescribed by ISO 27001. ***(4 Marks, November 2014)***

Answer

The four phases of Information Security Management System (ISMS) prescribed by ISO 27001 are as follows:

- **The Plan Phase –** This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
- **The Do Phase –** This phase includes carrying out everything that was planned during the previous phase.
- **The Check Phase –** The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.
- **The Act Phase –** The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The cycle of these four phases never ends, and all the activities must be implemented cyclically in order to keep the ISMS effective.

8
Emerging Technologies

Question 1

Discuss some of the pertinent objectives in order to achieve the goals of Cloud Computing.

(6 Marks, November, 2014)

Answer

Some of the pertinent objectives in order to achieve the goals of Cloud Computing are as follows:

- To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;
- To access services and data from anywhere at any time;
- To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;
- To consolidate IT infrastructure into a more integrated and manageable environment;
- To reduce costs related to IT energy/power consumption;
- To enable or improve "Anywhere Access" (AA) for ever increasing users; and
- To enable rapidly provision resources as needed.

Questions Based on the Case Studies

Question 1

ASK International proposes to launch a new subsidiary to provide e-consultancy services for organizations throughout the world, to assist them in system development, strategic planning and e-governance areas. The fundamental guidelines, programmes modules and draft agreements are all preserved and administered in the e-form only.

The company intends to utilize the services of a professional analyst to conduct a preliminary investigation and present a report on smooth implementation of the ideas of the new subsidiary. Based on the report submitted by the analyst, the company decides to proceed further with three specific objectives (i) reduce operational risk, (ii) increase business efficiency and (iii) ensure that information security is being rationally applied. The company has been advised to adopt BS 7799 for achieving the same.

(a) What are the two primary methods through which the analyst would have collected the data ?

(b) To retain their e-documents for specified period, what are the conditions laid down by Section 7, Chapter III of Information Technology Act, 2000? ***(5 Marks each, May 2010)***

Answer

(a) Two primary methods through which the analyst would have collected the data are given as follows:

(1) **Reviewing internal documents:** The analyst first tries to learn about the organization involved in or affected by the project. For example, to review an inventory system proposal, s/he will try to know 'how the inventory department operates' and 'who are the managers and supervisors'. S/he will examine organization charts and written operating procedures.

(2) **Conducting interviews:** Written documents tell the analyst 'how the system should operate' but they may not include enough details to allow a decision to be made about the merits of a system proposal nor do they present users' views about current operations. To learn these details, analysts use interviews. Preliminary investigation interviews involve only management and supervisory personnel.

(b) Section 7, Chapter III of Information Technology Act, 2000 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

(i) The information therein remains accessible so as to be usable subsequently.

(ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.

(iii) The details which will facilitate the identification of the origin, destination, dates and time of dispatch or receipt of such electronic record are available therein.

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

Moreover, this section does not apply to any law that provides for the retention of documents, records or information in the form of electronic records.

Question 2

ABC Industries Ltd., a company engaged in a business of manufacture and supply of automobile components to various automobile companies in India, had been developing and adopting office automation systems, at random and in isolated pockets of its departments.

The company has recently obtained three major supply contracts from International Automobile companies and the top management has felt that the time is appropriate for them to convert its existing information system into a new one and to integrate all its office activities. One of the main objectives of taking this exercise is to maintain continuity of business plans even while continuing the progress towards e-governance.

(a) When the existing information system is to be converted into a new system, what are the activities involved in the conversion process?

(b) What are the types of operations into which the different office activities can be broadly grouped under office automation systems?

(c) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity. ***(5 Marks each, November 2010)***

Answer

(a) Conversion from existing information system to a new system involves the following activities:

(i) Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually';

(ii) Performing data cleansing before data conversion;

(iii) Identifying the methods to assess the accuracy of conversion like record counts and control totals;

(iv) Designing exception reports showing the data which could not be converted through software; and

(v) Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

(b) Types of Operations:

The types of operations into which different office activities under Office Automation Systems can be broadly grouped, are discussed as under:

(i) **Document capture:** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.

(ii) **Document Creation:** This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.

(iii) **Receipts and Distribution**: This basically includes distribution of correspondence to designated recipients.

(iv) **Filling, Search, Retrieval and Follow-up:** This is related to filling, indexing, searching of documents, which takes up significant time.

(v) **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.

(vi) **Recording Utilization of Resources:** This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

(c) Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

(i) **Business resumption planning** – The Operation's piece of business continuity planning;

(ii) **Disaster recovery planning** – The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.

(iii) **Crisis Management** – The overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

Question 3

XYZ Industries Ltd., a company engaged in a business of manufacturing and supply of electronic equipments to various companies in India. It intends to implement E-Governance system at all of its departments. A system analyst is engaged to conduct requirement analysis and investigation of the present system. 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 and reliable. The company is relying on Information Technology for information and transaction processing. It is also presumed that the company is up and running all the time on 24 x 7 basis. Hence, the company has decided to implement a real time ERP package, which equips the enterprise with necessary capabilities to integrate and synchronize the isolated functions into streamlined business processes in order to gain a competitive edge in the volatile business environment. Also, the company intends to keep all the records in digitized form.

(a) What do you mean by system requirement analysis? What are the activities to be performed during system requirement analysis phase?

(b) What is the provision given in Information Technology Act 2000 for the retention of electronic records? ***(5 Marks each, May, 2011)***

Answer

(a) System requirements analysis is a phase, which includes a thorough and detailed understanding of the current system, identification of the areas that need modification/s to solve the problem, the determination of user/managerial requirements and to have fair ideas about various system development tools.

The following 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 requirements in terms of various parameters like completeness, consistency, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like- interviewing, research/document collection, questionnaires, observation;
- To develop models to document Data Flow Diagrams, E-R diagrams; and
- To document activities such as interviews, questionnaires, reports etc. and development of a system dictionary to document the modeling activities.

The document/deliverable of this phase is a detailed system requirements report, which is generally termed as SRS.

(b) Retention of Electronic Records: [Section 7] of IT Act 2000

The provision for the retention of electronic records is discussed in Section 7 of ITAA 2008, which is given as follows:

(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.

Question 4

ABC Udyog, a leading automobile company is having several manufacturing units, located in different parts of the world and manufacturing several types of automobiles. The units are working on legacy systems using an internet and collating information, but using different software and varied platforms (Operating Systems) which do not allow communication with each other. This results in huge inflow of duplicate data.

The company wishes to centralize and consolidate the information flowing from its manufacturing units in a uniform manner across various levels of the organizations, so that the necessary data required for preparing MIS reports, budget, and profit/loss accounts etc. could be available timely.

The company decided to engage XYZ consultancy Services for the development of new system. Being a Senior Project Leader of the Consultancy Services, you are entrusted with the responsibilities of handling this project.

Read the above carefully and answer the following with justifications:

(a) What areas are required to be studied in order to know about the present system? Write the problems that the ABC Udyog is presently facing.

(b) What are various backup techniques? Which backup technique, you will recommend and why? ***(5 Marks each, November 2011)***

Answer

(a) The following are the major areas, which should be studied in depth in order to understand the present system:

(i) **Review historical aspects**: A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts shall identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments.

(ii) **Analyze inputs:** A detailed analysis of the 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.

(iii) **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.

(iv) **Review methods, procedures and data communications:** A system analyst also needs to review and understand the present data communications used by the organization. S/he must review the types of data communication equipments, including data interface, data links, modems, dial-up and leased lines and multiplexers.

(v) **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'.

(vi) **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.

(vii) **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.

(viii) **Undertake overall analysis of present 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.

Presently, ABC Udyog is facing the following major problems:

- The company having its branches all over the world, is engaged in manufacturing of several types of automobiles. The units are working on legacy systems using an internet and collating information. Each unit is using different type of software on

varied platforms (operating systems), therefore, *they are not able to communicate with each other.* Because of this reason, *there is a huge inflow of data which could not be consolidated for analysis.*

- Lack of communication among units has resulted *into duplication of the data entry,* which is very costly. In addition, *timely availability of necessary and relevant data* required for the preparation of MIS Reports, budget, profit/loss account etc. is another important concern in the present system.
- It is confronted with the problem of *centralizing and consolidating the information flowing in from its various units* in uniform manner across various levels of the organization. Hence, there is an urgent need of a system that would entrust the company to address these important issues.

(b) Various back-up techniques are described as follows:

(i) **Full Backup:** A full backup captures all the files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.

(ii) **Incremental Backup:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

Normally, incremental backup are very difficult to restore. You will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

(iii) **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.

(iv) **Mirror back-up:** A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

In the present system, we recommend incremental backup because ABC Udyog has manufacturing units working on the legacy systems. Secondly, incremental backup is the

most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space, which is the current need of the automobile company.

Question 5

ABC is a leading company in the manufacturing of food items. The company is in the process of automation of its various business processes. During this phase, technical consultant of the company has highlighted the importance of information security and has suggested to introduce it right from the beginning. He has also suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risk. For carrying out all these suggestions, various best practices have been followed by the company. In addition, after each activity, appropriate standards' compliances have been tested to check the quality of each process. Various policies related with business continuity planning and disaster recovery planning have been implemented to ensure three major expectations from the software, namely, resist, tolerate and recover.

Read the above carefully and answer the following:

(a) What are the major suggestions given by the technical consultant? How the company is implementing these suggestions?

(b) Out of various types of plans used in business continuity planning, discuss recovery plan in brief.

(c) What should be the major components of a good information security policy, as per your opinion? ***(5 Marks each May 2012)***

Answer

(a) During the automation of various processes of ABC Company, the technical consultant of the company has given the following major suggestions:

- By realizing the importance of information security, he suggested to introduce it *right from the beginning*.
- In addition, he also suggested performing the risk assessment activity.
- Finally, he advised to mitigate the assessed risk.

For the implementation of all the above mentioned suggestions, the company took the following steps:

- The company followed various best practices for each process for the proper implementation of the suggestions.
- In addition, the company also tested the compliance of appropriate standards' after each activity, to check the quality of each process.

- Further, the company also implemented the policies related to business continuity planning and disaster recovery to ensure three broad expectations from the software: resist, tolerate and recover.

(b) **Recovery Plan:** The backup plan is intended to restore operations quickly so that the information system function can continue to service an organization, whereas, *recovery plans set out procedures to restore full information system capabilities.* Recovery plans should identify a recovery committee that will be responsible for working out the specification of the recovery to be undertaken.

The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate '*which applications are to be recovered first'*. Members of a recovery committee must understand their responsibilities. Here, there is a major issue that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice for executing their responsibilities so that they are prepared for a disaster. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

(c) A good Information 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 (BCP),
- Legal compliances,
- Monitoring and auditing requirements, and
- Underlying technical policy.

Question 6

ABC Appliances Limited is a popular marketing company, which has many branches located in different places. It does all its business activities such as receiving orders, placing orders, payments, receipts etc. through online. With increased business activities, the company faces several problems with the existing information system. It realizes that the existing system is outdated and needed improvement. Hence, it wishes to enhance the existing system with adequate measures for information security in order to ensure the smooth functioning of new information system and protect the company from loss or embarrassment caused by security failures. To develop such a new system, the company has formed a system development team with professionals like project managers, system analysts and system designers. The team has executed all the phases involved in the SDLC and implemented the new system successfully. Finally, the Post Implementation Review has also been conducted to determine whether the new system adequately meets present business requirements and the company is satisfied with the PIR report.

Read the above carefully and answer the following:

(a) State the advantages of SDLC from the perspective of the IS Audit.

(b) What are the activities to be undertaken during the Post Implementation Review?

(5 Marks each November 2012)

Answer

(a) From the perspective of the IS Audit, the following are the major advantages of SDLC:

- The IS Auditor can have the 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/her examination, can state in his/her report about the compliances by the IS management of the procedures, if any, set up by the management.
- The IS Auditor, if has a technical knowledge and ability of the area/s of SDLC, can be a guide during various phases of SDLC.
- The IS Auditor can provide an evaluation of the methods and techniques used during various development phases of the SDLC.

(b) During the Post Implementation Review, the team should, according to their terms of reference, review:

- the main functionality of the operational system against the User Requirements Specification along with the confirmation that all the anticipated benefits, both tangible and intangible, have been delivered;
- system performance and operation;
- the development techniques and methodologies employed;

- estimated time-scales and budgets, and identify reasons for variations, if any;
- changes to requirements, and confirm that they were considered authorized and implemented in accordance with change and configuration management standards; and
- the findings, conclusions and recommendations documented in a report for the authorizing authority to consider.

Question 7

XYZ Company is a retail chain house having many branches located in different places for its operation. Its business processes are cumbersome and tedious as it has multiple sources of procurement and supply destinations.

The CEO of company feels that existing information system does not meet its present requirements. He seeks for high end solution to stream line and integrate its operation processes and information flow to synergize all its major resources. Further he expects that the new system should provide a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable information. The company follows the best practices of System Development Life Cycle (SDLC), which consists of various phases starting from preliminary investigation till post implementation review, controls and security aspects.

The CEO of the company appoints a committee of three persons, one of them is IT expert, second one is security expert and third one is company's auditor to suggest the followings:

(a) List the activities to be performed during the phase of System Requirement Analysis.

(b) What boundary control techniques should be used in user control?

(5 Marks each, May 2013)

Answer

(a) The activities to be performed during the phase of System Requirements Analysis are given as follows:

- To identify and consult the stakeholders to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine their 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 the activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and

- To document the activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

The final deliverable of this phase of SDLC is SRS.

(b) The major controls of the boundary system are the access control mechanisms. Access controls are implemented with an access control mechanism and links the authentic users to the authorized resources for which they are permitted to access. The access control mechanism has three steps, identification, authentication and authorization with respect to the access control policy.

Major boundary control techniques are given as follows:

- **Cryptography**: It deals with programs for transforming data into codes that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).
- **Passwords**: User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.
- **Personal Identification Numbers (PIN)**: PIN is similar to a password assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm, or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN or a digital signature are exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- **Identification Cards**: Identification cards are used to store information required in an authentication process. These cards used to identify a user, are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
- **Biometric devices**: Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

Question 8

Skyair is an airline company operating with in-house developed software till now. Its profit margins are under pressure due to inefficiency and disorganized work culture.

To survive in the highly competitive environment, it has to improve the efficiency of its internal processes and synchronize isolated functions into streamlined business processes so that work culture is improved. Hence it has decided to purchase and implement a real time ERP package. In order to improve its margin, it wants to transact with suppliers and customers electronically and maintain all records in electronic form. Security of information is a key activity of this process which must be taken care of from the beginning. As a member of implementation team you are required to answer the following:

(a) What issues you would like to raise during the technical feasibility of new proposed system?

(b) Describe the provisions for authentication of electronic records under Information Technology (Amendment) Act, 2008.

(c) Describe any five major types of information security policy which company must maintain to meet the security objectives. ***(5 Marks each, November 2013)***

Answer

(a) During the technical feasibility of new proposed system, the following issues may be raised:

- Does the necessary technology exist to do 'what is suggested (and can it be acquired)'?
- Does the proposed equipment/s have the technical capacity to hold the data required to be used by the new system?
- Can the proposed application be implemented with existing technology?
- Will the proposed system provide the adequate responses to inquiries, regardless of the number or location of users?
- Can the system be expanded, if developed?
- Are there technical guarantees of accuracy, reliability, ease of access, and data security?

(b) Provisions of authentication of electronic records are given under Section 3 of Information Technology (Amendment) Act, 2008, which is given as follows:

***[Section 3]* Authentication of Electronic Records:**

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

(c) Major Information Security Policies, which company must maintain to meet the security objectives, are given as follows:

- **Information Security Policy:** This policy provides a definition of Information Security, its overall objective and the importance applies to all users.
- **User Security Policy:** This policy sets out the responsibilities and requirements for all IT systems' users. It provides security terms of reference for Users, Line Managers and System Owners.
- **Acceptable Usage Policy:** This sets out the policy for acceptable usage of email and Internet services.
- **Organizational Information Security Policy:** This policy sets out the Group policy for the security of its information assets and the IT systems, processing this information.
- **Network & System Security Policy:** This policy sets out detailed policy for system and network security and applies to IT department users.
- **Information Classification Policy:** This policy sets out the policy for the classification of information.
- **Conditions of Connection:** This policy sets out the Group policy for connecting to their network. It applies to all organizations connecting to the Group and relates to the conditions that apply to different suppliers' systems.

Question 9

*Software development is an integrated process spanning the entire **IT** organization. ABC Technologies Ltd. is a leading company in the field of software development of various domain. The company is committed to follow System Development Life Cycle (SDLC) with best practices for its different activities. A system development methodology is a formalized,*

standardized, documented set of activities that analysts, designer and user can come out to develop and implement an information system which contains appropriate controls for all its phases so as to retain records in electronic format with reasonable level of security.

Read the above carefully and answer the following:

(a) As a part of system development team, the system analyst prepare a document called the System Requirement Specification" (SRS). Describe the contents of SRS for a typical software development.

(b) Describe the provisions for retention of electronic records under Section 7 of Information Technology (Amendment) Act, 2008.

(c) Explain the role of auditor in information processing system design through SDLC.

(5 Marks each, May 2014)

Answer

(a) Major contents of a System Requirements Specification (SRS) for a typical software development are given as follows:

- **Introduction:** It contains goals and objectives of the software in the context of computer-based system and information description.
- **Information Description:** It contains 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 are the major parts of functional description.
- **Behavioral Description:** It covers responses to external events and internal controls.
- **Validation Criteria:** It contains classes of tests to be performed to validate functions, performance and constraints.
- **Appendix:** It may have various items like 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 understanding of the development team about the existing processes. Only after ensuring that the document represents existing processes accurately, the user should sign the document. This is a technical requirement of the contract between users and development team / organization.

(b) Provisions of retention of electronic records under Section 7 of Information Technology (Amendment) Act, 2008 are given as follows:

[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.

(c) The role of auditor in information processing systems' design is given as follows:

- To evaluate the appropriateness of the requirements elicitation strategy in the scope of the stakeholders and the quality of the requirements document.
- To ensure that the system design needs to capture all data/information flow within the system.
- To evaluate the structure of the database design and cost of the data model.
- User interface is the source of user interactivity with the system and is a critical activity. Auditor should verify that the design and quality of the interface are following the best design practices.
- To assess the efficiency of the tasks assigned to the appropriate hardware and software resources of the physical design of the system. The performance of a critical system should also be evaluated with the help of simulations.

Question 10

XYZ Limited is a multinational company engaged in providing financial services worldwide. Most of the transactions are done online. Their current system is unable to cope up with the growing volume of transactions. Frequent connectivity problems, slow processing and a few

instances of phishing attacks were also reported. Hence the Company has decided to develop a more robust in-house software for providing good governance and sufficient use of computer and IT resources. You, being an IS auditor, has been appointed by the Company to advise them on various aspects of project development and implementation. They want the highest levels of controls in place to maintain data integrity and security with zero tolerance to errors.

The Company sought your advise on the following issues:

(a) What are the major data integrity policies you would suggest?

(b) What are the categories of tests that a programmer typically performs on a program unit?

(c) Discuss some of the critical controls required in a. computerized environment.

(d) What are your recommendations for efficient use of computer and IT resources to achieve the objectives of 'Green Computing'? ***(5 Marks each, November 2014)***

Answer

(a) Major data integrity policies are given as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **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.
- **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.

(b) There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows:

- **Functional Tests:** Functional Tests check 'whether programs do, what they are supposed to do or not'. The test plan specifies operating conditions, input values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.
- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
- **Stress Tests:** 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. The purpose of a stress test is to determine the limitations of the program.

- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

(c) Some of the critical controls required in a computerized environment are as follows:

- Management understanding of Information System risks and related controls;
- Presence or adequate Information System control framework;
- Presence of general controls and Information System controls;
- Awareness and knowledge of Information System risks and controls amongst the business users and even IT staff;
- Implementation of controls in distributed computing environments and extended enterprises;
- Control features or their implementation in highly technology driven environments; and
- Appropriate technology implementations or adequate security functionality in technologies implemented.

(d) Some recommendations for efficient use of computer and IT resources to achieve the objectives of 'Green Computing' are as follows:

- Power-down the CPU and all peripherals during extended periods of inactivity.
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times.
- Power-up and power-down energy-intensive peripherals such as laser printers according to need.
- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
- Use notebook computers rather than desktop computers whenever possible.
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity.
- Minimize the use of paper and properly recycle waste paper.
- Dispose of e-waste according to central, state and local regulations.
- Employ alternative energy sources for computing workstations, servers, networks and data centers.