COMPILATION OF SUGGESTED ANSWERS TO QUESTIONS SET IN THE INSTITUTE'S EXAMINATIONS MAY, 2010 – MAY, 2017

PAPER-6
INFORMATION SYSTEMS CONTROL & AUDIT

Created By : CA Vidit Todi

Chapter 1: Concepts of Governance and Management of Information Systems

Q1. Explain the major functions of the IT Steering Committee? **(May 2017)**

Ans. The major functions of the IT Steering Committee would include the following:

- ♦ To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- ♦ To establish size and scope of IT function and sets priorities within the scope;
- ♦ To review and approve major IT deployment projects in all their stages;
- ♦ To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- ♦ To review the status of Information Systems' plans and budgets and overall IT performance;
- ♦ To review and approve standards, policies and procedures;
- ♦ To make decisions on all key aspects of IT deployment and implementation;
- ♦ To facilitate implementation of IT security within enterprise;
- ♦ To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- ♦ To report to the Board of Directors on IT activities on a regular basis.

Q2. Discuss in brief any 6 key practices for assessing and evaluating the system of Internal Control in an enterprise. OR 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? **(May 2017, Nov 2014)**

Ans. The key practices for assessing and evaluating the system of internal controls in an enterprise are as follows:

- ♦ **Monitor Internal Controls:** Continuously monitor, benchmark & 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.

Q3. What are the key benefits of GEIT? **(May 2017, May 2016)**

Ans. Benefits of Governance of Enterprise IT (GEIT) are as follows:

- ♦ It provides a consistent approach integrated and aligned with the enterprise governance approach.
- ♦ It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.
- ♦ It ensures that IT-related processes are overseen effectively and transparently.
- ♦ It confirms compliance with legal and regulatory requirements.
- ♦ It ensures that the governance requirements for board members are met.

Q4. What are the enablers described by COBIT 5 Framework? **(Nov 2016, May 2014)**

Ans. The COBIT 5 framework describes seven categories of enablers which are as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **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.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.
- **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.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **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.

Q5. What is IT Governance? What are the key practices which determine the status of IT governance in the enterprise? **(Nov 2016)**

Ans. **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. The objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT. In other words, IT Governance is the system by which IT activities in a company or enterprise are directed and controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs.

Key practices to determine status of IT Governance are as follows:

- Who makes directing, controlling and executing decisions?

- How the decisions are made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How exceptions are handled?
- How the governance results are monitored and improved?

Q6. 'IT has to provide critical inputs to meet the information needs of all the stakeholders'. Define IT Governance and list out its benefits. OR Describe the key benefits of IT Governance achieved at highest level in an organization. **(Nov 2016, Nov 2015, Nov 2014)**

Ans. One of the well-known definitions of IT Governance is that "IT Governance is the system by which IT activities in a company or enterprise are directed and controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs".

The key benefits of IT Governance which are achieved by implementing/improving governance or management of enterprise, at the highest level in an organization are as follows:

- 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.

Q7. What are the key management practices which are required for aligning IT Strategy with Enterprise Strategy? **(May 2016, May 2015)**

Ans. The key management practices which are required for aligning IT strategy with enterprise strategy are as follows:

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.
- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.

- **Define the strategic plan and road map:** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

Q8. Write a short note on Risk Management Strategies. **(May 2016)**

Ans. Risk management strategies are as below:

- **Tolerate/Accept the risk:** One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk:** It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the risk:** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.
- **Treat/mitigate the risk:** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back:** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

Q9. What is the role of IT in enterprises? Explain the different levels of managerial activity in an enterprise. **(Nov 2015)**

Ans. Role of IT in Enterprises is as under:

- In an increasingly digitized world, enterprises are using IT not merely for data processing but more for strategic and competitive advantage too. IT deployment has progressed from data processing to MIS to Decision Support Systems to online transactions/services.
- IT has not only automated the business processes but also transformed the way business processes are performed. IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.
- The extent of technology deployment not only impacts the way internal controls are implemented in an enterprise but also provide better and innovative services from strategic perspective.
- An IT strategy aligned with business strategy ensures the value creation and facilitates benefit realization from the IT investments.
- Extensive organization restructuring or Business Process Re-Engineering may be facilitated through IT deployments.

The different levels of managerial activity in an enterprise are as under:

- **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. It is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved.
- **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
- **Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

Q10. Briefly describe the key management practices provided by COBIT for ensuring IT compliances. **(Nov 2015)**

Ans. COBIT 5 provides key management practices for ensuring IT compliance with external compliances as relevant to the enterprise. The practices are given as follows:

- **Identify External Compliance Requirements:** On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.
- **Optimize Response to External Requirements:** Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and best practice guidance for adoption and adaptation.
- **Confirm External Compliance:** Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.
- **Obtain Assurance of External Compliance:** Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

Q11. Write a short note on Metrics of risk management. **(Nov 2015)**

Ans. **Metrics of Risk Management:** Enterprises have to monitor the processes and practices of IT risk management by using specific metrics. Some of the key metrics are as follows:

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk Assessment;
- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

Q12. The Management of IT related risks is a key part of Enterprise Governance. Name the key management practices to achieve this objective. **(May 2015)**

Ans. The key Management Practices for implementing IT Risk Management are given as follows:

- **Collect Data:** To enable effective IT related risk identification, analysis and reporting.
- **Analyze Risk:** To develop useful information to support risk decisions.
- **Maintain a Risk Profile:** To maintain an inventory of known risks and risk attributes.
- **Articulate Risk:** To inform IT- related exposures and opportunities to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** To manage opportunities and reduce risk to an acceptable level as a portfolio.

- **Respond to Risk:** To respond limit the magnitude of loss from IT related events in a timely manner.

Q13. Write short notes on the following:
(a) Principles of COBIT 5
(b) Vulnerability **(May 2015)**

Ans.

(a) **Principles of COBIT 5**

- **Principle 1: Meeting Stakeholder Needs -** COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. An enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific; IT related goals and mapping these to specific processes and practices.
- **Principle 2: Covering the Enterprise End-to-End -** COBIT 5 integrates governance of enterprise IT into enterprise governance. COBIT 5 covers all functions and processes within the enterprise and considers all IT related governance and management enablers to be enterprise-wide and end-to-end.
- **Principle 3: Applying a Single Integrated Framework -** COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allowing the enterprise to use COBIT 5 as the overarching governance and management framework integrator.
- **Principle 4: Enabling a Holistic Approach -** COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT that require a holistic approach, taking into account several interacting components.
- **Principle 5: Separating Governance from Management -** The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

(b) **Vulnerability:** Vulnerability is the weakness in the system safeguards that exposes the system to threats and can be exploited by the attackers. The weakness may be in information system/s, cryptographic systems or other components e.g. system security procedures, hardware design, internal controls that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.

Some examples of vulnerabilities are as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

In other words, Vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

- 'Allows an attacker to execute commands as another user'
- 'Allows an attacker to access data that is contrary to the specified access restrictions for that data'
- 'Allows an attacker to pose as another entity'
- 'Allows an attacker to conduct a denial of service'.

Q14. Write short note on the following:
(a) Internal Controls as per COSO. **(Nov 2014, Nov 2012)**
(b) Risk, Vulnerability and Threat **(Nov 2014)**

Ans. (a) 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.

(b) **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.

Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.

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.

Q15. Write a short note on Risk Assessment. **(May 2014, May 2013)**

Ans. **Risk Assessment:** Risk assessment is a step in the risk management procedure. Risk assessment is the determination of quantitative or qualitative value of the risk related to a concrete situation and a recognized threat. A risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters.

Risk assessment is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well-tested contingency plan. 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.

Chapter 2: Information Systems Concepts

Q1. What are the major limitations of a Management Information System? **(May 2017, Nov 2012)**

Ans. Major Limitations of Management Information Systems (MIS) are 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 the purpose of 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 types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- ♦ The effectiveness of MIS is reduced in enterprises, where the culture of hoarding information and not sharing with other holds.
- ♦ MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

Q2. What are the important implications of an MIS in business? **(May 2017)**

Ans. Following are some of the important implications of Management Information Systems (MIS) in business:

- ♦ MIS supports the managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill the organizational goals.
- ♦ An organization can survive and thrive in a highly competitive environment on the strength of a well-designed Management Information system that provides flexible and speedy access to accurate data.
- ♦ MIS helps in making right decision at the right time i.e. just on time.
- ♦ A good MIS may help in generating innovative ideas for solving critical problems.
- ♦ Knowledge gathered though MIS may be utilized by managers in unusual situations.
- ♦ MIS may be viewed as a process; it can be integrated to formulate a strategy of action or operation.
- ♦ MIS provides reports to management that can help in making effective, structured types as applicable to decisions of day-to-day operations.

Q3. "Information has become a key resource for any type of business activity." Define the term "Information" and briefly discuss the various attributes of information. **(May 2017, Nov 2011)**

Ans. **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 -** Information is useless if it is not available at the time of need. Database is a collection of files which is collection of records and data from where the required information is derived for useful purpose.
- **Purpose/Objective -** Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data. 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 understandable by the people and may be in the form of voice, text and combination of these two. Format design should be simple, relevant and should highlight important point in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information, the different formats can be used e.g. diagrams, graphs, curves are best suited for representing the statistical data.
- **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 interval of time so that the current score will be available.
- **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- the information available from internet site should be available at a click of mouse.
- **Frequency -** The frequency with which information is transmitted or received affects its value. For example- the weekly reports of sales show little change as compared to the quarterly and contribute less for accessing 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 find 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 supports in evaluating his performance.
- **Quality -** It means the correctness of information. For example, an over-optimistic manager may give too high estimates of the profit of product which may create problem in inventory and marketing.
- **Transparency -** It is essential in decision and policy making. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.
- **Value of Information -** It is defined as difference between the value of the change in decision behaviour 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.

Q4. Discuss the pre-requisites of an effective MIS. **(Nov 2016, May 2014)**

Ans. The pre-requisites of an effective Management Information Systems (MIS) are as follows:

- **Database -** It is collection of files, which is collection of records and records are nothing but collection of data. The data in database is organized in such a way that accessing to the data is improved and redundancy is reduced. The main characteristics of database are given as follows:
  - 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 Database Management System (DBMS).
- **Qualified System and Management Staff -** The second pre-requisite of effective MIS is that it should be manned by qualified officers. These officers, who are experts in the field, should understand clearly the views of their fellow officers. For this, the organizational management base should comprise of two categories of officers - Systems and Computer Experts and Management experts.
  - Systems and Computer experts in addition to their expertise in their subject area/s should also 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 should also understand quite clearly the concepts and operations of a computer. This basic knowledge of computers will be useful to place them in a comfortable position, while working with systems technicians in designing or otherwise of the information system.
- **Support of Top Management -** The support from top management is required for the effectiveness of MIS in an organization. The reasons for the same are as follows:
  - Any implementation, which does not receive the support of top management will not be effectively controlled and tends to get lesser priority and may be delayed or abandoned.

- The resources involved in computer-based information systems are large and are growing larger in view of importance gained by management information system.
- To gain the support of top management, the officers should place before top management all the supporting facts and state clearly the benefits, which will accrue from it to the concern. This step will certainly enlighten management, and will change their attitude towards MIS. Their wholehearted support and cooperation will help in making MIS an effective one.

o **Control and maintenance of MIS -** Control of the MIS means the operation of the system as it was designed to operate. Some time, 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 devise checks for the information system control. Maintenance is closely related to control. Formal methods for changing and documenting changes must be provided.

Q5. "The intuitive character of executive decision making is reflected strongly in the types of information found most useful to executives". Discuss characteristics of the types of information used in executive decision making. **(Nov 2016)**

Ans. "The intuitive character of executive decision-making is reflected strongly in the types of information found most useful to executives". The characteristics of the types of information used in executive decision making are as follows:

o **Lack of structure –** Many of the decisions made by executives are relatively unstructured. These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance. Also, it is not always obvious, 'which data are required' or 'how to weigh available data when reaching a decision.'

o **High degree of uncertainty –** Executives work in a decision space that is often characterized by a lack of precedent. For example, when the Arab oil embargo hit in mid 1970s, no such previous event could be referenced for advice. Executives also work in a decision space where results are not scientifically predictable from actions. If prices are lowered, for instance, product demand will not automatically increase.

o **Future orientation –** Strategic-planning decisions are made to shape future events. As conditions change, enterprises must change also. It is the executive's responsibility to make sure that the organization keeps pointed toward the future. Some key questions about the future include: "How will future technologies affect what the company is currently doing? What will the competition (or the government) do next? What products will consumers demand five years from now?" As one can see, the answers to these questions about the future external environment are vital.

o **Informal Source –** Executives, more than other types of managers, rely heavily on informal source for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Informal sources such as television might also feature news of momentous concern to the executive – news that he or she would probably never encounter in the company's database or in scheduled computer reports.

- **Low level of detail –** Most important executive decisions are made by observing broad trends. This requires the executive to be more aware of the large overview than the tiny items. Even so, many executives insist that the answers to some questions can only be found by mucking through details.

Q6. What are the IT tools you consider critical for business growth? **(May 2016, Nov 2014)**

Ans. Some of the IT tools critical 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 –** Through Internet, 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.

Q7. Write a short note on Components of ERP. **(May 2016)**

Ans. Components of Enterprise Resource Planning (ERP) are listed below:

(i) **Software Component:** The software component is the component that is most visible part and consists of several modules such as Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligence.

(ii) **Process Flow:** It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model makes it easier to understand how ERP work.

(iii) **Customer mindset:** By implementing ERP system, the old ways for working which user understand and comfortable with have to be changed and may lead to users' resistance. In order to lead ERP

implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.

(iv) **Change Management:** In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.

Q8. 'MIS supports the managers at different levels to take decisions to fulfill the organizational goals.' Explain the major characteristics of MIS to achieve these goals. **(Nov 2015, Nov 2013)**

Ans. 'Management Information System (MIS) supports the managers at different levels to take decisions to fulfill the organizational goals.' The major characteristics of MIS to achieve these goals are 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 as well.
- **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 their sufficient 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:** MIS has an integrated approach as all the functional and operational information subsystems are 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 subsystems 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 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 period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
- **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 by developing 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 management information system.

Q9. As a member of IS Steering Committee, how do you classify the information for better integrity and security? **(Nov 2015)**

Ans. As a member of IS Steering Committee, the Information can be classified as under for better integrity and security:

- **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 etc., 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 be 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 be minimal.

Q10. What is the need for an expert system in an organization? What are its benefits?
(Nov 2015, Nov 2010)

Ans. Major reasons for the need of Expert Systems are as follows:

- Expert labor is expensive and scarce. Knowledge workers/employees, who routinely work with data and information to carry out their day-to-day duties are not easy to find and keep and companies are often faced with a shortage of talent in key positions.
- Moreover, no matter how bright or knowledgeable certain people are, they often can handle only a few factors at a time.
- Both these limitations imposed by human information processing capability and the rushed pace at which business is conducted today put a practical limit on the quality of human decision making this putting a need for expert systems.

The key benefits of Expert Systems are given below:

- 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 it can be summoned almost as a real-life expert might be summoned.
- Expert Systems assist novices in thinking the way experienced professional 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.

Q11. Write a short note on Components of ERP model. **(Nov 2015)**

Ans. The components of ERP Model are as below:

(i) **Software Component:** The software component is the component that is most visible part and consists of several modules such as Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligent.

(ii) **Process Flow:** It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model, makes it easier to understand how ERP work.

(iii) **Customer mindset:** By implementing ERP system, the old ways for working which user understand and comfortable with need to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellence job without help from ERP system. In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.

(iv) **Change Management:** In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.

Q12. What are the important implications of Information Systems in business? **(May 2015)**

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

- Information system helps managers in efficient decision-making to achieve the 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 helps 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 system may be utilized by managers in unusual situations.
- Information system is viewed as a process; it can be integrated to formulate a strategy of action or operation.

Q13. Office Automation Systems (OAS) is the most rapidly expanding system. Describe the broad groups of OAS based on the types of its operations. **(May 2015)**

Ans. Office Automation Systems (OAS) is most rapidly expanding computer based information systems. The broad groups that can be formed on the basis of its operations are as follows:

(i) **Text processing system:** The text processing system automates the process of document capture and/ or creation of new documents such as letters, reports, memo etc. This permits use of standard stored information to produce personalized documents. It reduces effort and minimizes the chances of errors.

(ii) **Electronic Document Management system:** It captures the information contained in documents, stored for future reference and makes them available to the users as and when required. These systems are very helpful in remote access of documents and internal communication through network. It also helps to keep record of resources utilization.

(iii) **Electronic message communication system:** The electronic message communication system helps in receipts and distribution of electronic records. It offers a lot of economy in terms of reduced time in sending or receiving the message; online development and editing; broadcasting and rerouting; and integration with other information system. E-mail, Fax, and voice mail are important OAS.

(iv) **Teleconferencing and Video Conferencing systems:** This OAS helps in receipt and distribution of information involving more than two persons located at two or more different places through audio or video with or without computer system.

Q14. State four major tasks performed by an Operating System while allowing users and their applications to share and access common resources. **(May 2015)**

Ans. Operating System is the computer control program that allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Some of the major tasks performed by an Operating system are as follows:

- **Scheduling Jobs:** They can determine the sequence in which jobs are executed, using priorities established.
- **Managing Hardware and Software Resources:** They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.
- **Maintaining System Security:** They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.
- **Enabling Multiple User Resource Sharing:** They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.
- **Handling Interrupts:** An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed. Interrupts are issued when a program requests an operation.
- **Maintaining Usage Records:** They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output devices.

Q15. A business manager should have adequate knowledge to operate Information Systems effectively. Elaborate. **(May 2015)**

Ans. To operate Information Systems (IS) effectively and efficiently, a business manager should have following knowledge about it.

- **Foundation Concepts –** It includes fundamental business, and managerial concepts e.g. 'what are components of a system and their functions', or 'what competitive strategies are required'.
- **Information Technologies (IT) –** It includes operation, development and management of hardware, software, data management, networks, and other technologies.
- **Business Applications –** It includes major uses of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.
- **Development Processes –** It comprise how end users and IS specialists develop and execute business/IT solutions to problems.
- **Management Challenges –** It includes 'how the function and IT resources are maintained' and utilized to attain top performance and build the business strategies.

Q16. 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. **(Nov 2014, May 2013)**

Ans. **Expert System -** An Expert System is highly developed Decision Support System that utilizes knowledge generally possessed by an expert to share 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? And so on.

Some of the properties that potential applications 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.

Q17. 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. **(May 2014)**

Ans. 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.

Q18. Define Transaction Processing System (TPS). List out the salient features of a TPS. **(Nov 2013)**

Ans. **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.

Q19. What general guidelines you would suggest before starting the implementation of ERP package? **(May 2013)**

Ans. The general guidelines, which are to be followed before starting the implementation of an ERP package, are given as follows:

- Understanding the corporate needs and culture of the organization and then adapt the implementation technique to match these factors;
- Doing a business process redesign exercise prior to starting the implementation;
- Establishing a good communication network across the organization;
- Providing a strong and effective leadership so that people down the line are well motivated;
- Finding an efficient and capable project manager;
- Creating a balanced team of implementation consultants, who can work together as a team;
- Selecting a good implementation methodology with minimum customization;
- Training end users; and
- Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

Q20. How does Executive Information System differs from Traditional Information System? **(May 2013)**

Ans. 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	Available	Not available

Information format	Text with graphics	Tabular
Nature of interface	User-friendly	Computer-operator

Q21. What is meant by EIS? What are its characteristics? **(Nov 2012, May 2011)**

Ans. **Executive Information System (EIS):** An EIS – sometimes also referred as an Executive Support System (ESS) is a DSS that is designed to meet the special needs of top-level managers. Some people use the terms "EIS" and "ESS" inter changeably. Any distinction between the EIS and ESS usually is because Executive Support Systems are likely to incorporate additional capabilities such as electronic mail etc.

Some of the important characteristics of EIS are given as follows:

- EIS is a Computer based information system that serves the information needs 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 tools like trend analysis, market conditions etc.
- EIS can easily provide a DSS support for decision making.

Q22. Explain any four features of Electronic Mail. **(Nov 2012)**

Ans. 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.

Q23. What is Decision Support System? Discuss its characteristics in brief. **(May 2012)**

Ans. 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.

Q24. Discuss the constraints in operating a MIS. **(May 2012)**

Ans. 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.

Q25. Discuss important characteristics of Computer based Information Systems in brief. **(May 2011)**

Ans. 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.

Q26. Write a short note on Business applications of Expert systems for Management Support systems. **(May 2011)**

Ans. 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.

Q27. What are the types of operations into which the different office activities can be broadly grouped under office automation systems? **(Nov 2010)**

Ans. **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.

Q28. Discuss some of the important advantages of Information Systems in business. **(May 2010)**

Ans. 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.

Chapter 3: Protection of Information Systems

Q1. Write short notes on following:

(a) Time Bomb vs. Logic Bomb **(May 2017)**

(b) Need of Boundary Controls and major boundary control techniques **(May 2017, May 2015, May 2013)**

Ans.

(a) **Time Bomb:** These are the programs that cause perverse activity, such as disruption of computer system, modifications, or destructions of stored information etc. on a date and time for which it has been developed. In other words, time bomb lies idle until some date or time triggers it. The computer clock initiates it.

Logic Bomb: These are the programs that are activated by combination of events. In other words, logic bombs lie idle until some specified circumstances trigger it. Once triggered, the bomb sabotages the system by destroying programs, data or both.

(b) Need of Boundary Controls:

The Boundary controls can be put in place that will establish interface between the user of the system and the system itself. The major controls of the boundary system are the access control mechanisms that links the authentic users to the authorized resources, they are permitted to access and thus are the line of control for intruders to gain access to the company's asset. The access control mechanism has three steps of Identification, Authentication and Authorization with respect to the access control policy implemented. The user can provide three factors of input information for the authentication process and gain access to his required resources.

Major Boundary Control techniques are as follows:

- **Cryptography:** It deals with programs for transforming data into cipher text 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.
- **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.
- **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database; independent to a user identification details, or a customer selected number. Hence, a PIN may be 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 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.

Q2. Explain the Impact/repercussions of Cyber Frauds on Enterprises. **(Nov 2016, Nov 2015)**

Ans. The impact of cyber frauds on enterprises 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 (Amendment) Act 2008, 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. There have been instances where share prices of such companies went down, as the news of such attack percolated to the market.
- **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.

Q3. What are the main characteristics of detective controls which are designed to detect errors, omissions or malicious acts that occur? **(Nov 2016)**

Ans. The main characteristics of Detective controls which are designed to detect errors, omissions or malicious acts that occur are as follows:

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

Q4. Discuss File Interrogation as one of the three levels of input validation controls. **(Nov 2016)**

Ans. Input validation controls are intended to detect errors in the transaction data before the data are processed. File Interrogation is one of the three levels of input validation controls.

- **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 be processed.
- **Internal and External Labeling:** Labeling of storage media is important to ensure that the proper files are loaded for process. 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 & availability. These controls ensure that correct file is used for processing.
- **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.

Q5. Operating System not only provides the platform for an application to use various IS resources but is also the last barrier to be conquered for unlimited access to all the resources. Explain the statement by describing any six operating system access controls to protect IS resources from unauthorised access. **(May 2016)**

Ans. Operating system not only provides the platform for an application to use various Information System resources but is also the last barrier to be conquered for unlimited access to all the resources. Hence, protecting operating system access is extremely crucial. Some of the common operating system access controls to protect IS resources from unauthorized access are as follows:

- **Automated terminal identification:** This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.
- **Terminal log-on procedures:** The log-on procedure does not provide unnecessary help or information, which could be misused by an intruder.
- **User identification and authentication:** The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.
- **Password management system:** An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
- **Use of system utilities:** System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- **Duress alarm to safeguard users:** If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.
- **Terminal time out:** Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
- **Limitation of connection time:** Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m.—or on a Saturday or Sunday.

Q6. Explain any four advantages of electronic door locks over bolting and combinational locks as a part of Physical Access Controls. **(May 2016)**

Ans. The following are the advantages of electronic door locks over bolting and combinational locks:

- Through the special internal code that is stored internally within the card; cards can be made to identify the correct individual.
- Individuals access needs can be restricted through the special internal code and sensor devices. Restrictions can be assigned to particular doors or to particular hours of the day.
- Degree of duplication is reduced.
- Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. If unauthorized entry is attempted silent or audible alarms can be automatically activated.
- An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also, parts of security. The card key becomes an important item to retrieve when an employee leaves the firm.

Q7. Write short notes on the following:

(a) Issues to be addressed by Information Security Policy. **(May 2016, May 2013)**
(b) Any four major impacts of Technology on Internal Controls. **(May 2016)**

Ans. (a) The Information Security 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.

(b) The impact of Technology on Internal Controls is as follows:

- **Competent and Trustworthy Personnel:** Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the persons responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations.
- **Segregation of Duties:** In a computerized system, the auditor should be concerned with the segregation of duties within the IT department. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output.
- **Authorization Procedures:** In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorization, e.g. a supervisor's signature, may be replaced by computerized authorization controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
- **Adequate Documents and Records:** In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available to trace the transactions in a computerized system. However, if the controls over the protection and storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.
- **Physical Control over Assets and Records:** Physical control over access and records is critical in both manual systems and computer systems. Computerized financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster. The nature and types of control available have changed to address these new risks.
- **Adequate Management Supervision:** In computer system, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried out remotely. The Management's supervision and review helps to deter and detect both errors and fraud.
- **Independent Checks on Performance:** If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.
- **Comparing Recorded Accountability with Assets:** Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented

to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.

- **Delegation of Authority and Responsibility:** A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users.

  Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

Q8. 'Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organisation'. What are the problems do you think that any organization can face with the result of computer crimes? **(Nov 2015)**

Ans. Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization. Computer crimes generally result in loss of customers, embarrassment to management and legal actions against the organizations. These are given as follows:

- **Financial Loss:** Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.
- **Legal Repercussions:** An organization has to adhere to many laws while developing security policies and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures.
- **Loss of Credibility or Competitive Edge:** In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.
- **Blackmail/Industrial Espionage:** By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** These events can spoil the reputation of the organization. Legal or regulatory actions against the company may be also a result of disclosure.
- **Sabotage:** People, who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities. They do it because of their dislike towards the organization or for their intemperance.
- **Spoofing:** A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. A penetrator makes the user think that s/he is interacting with the operating system. For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes the user login again.

Q9. What is meant by Information Security Policy? What are the components of a good security policy? **(Nov 2015, Nov 2013, May 2013, May 2012)**

Ans. An Information Security Policy may be defined as a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide. In its basic form, an information security policy is a document that describes an organization's information security controls and activities. The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business. An Information Security Policy is the essential foundation for an effective and comprehensive information security program. It is the primary way

in which management's information security concerns are translated into specific measurable and testable goals and objectives. It provides guidance to the people, who build, install, and maintain information systems.

Components of a good Security Policy:

A good security policy should clearly state the following:

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

Q10. Explain briefly major ways to control remote and distributed data processing in the new Web Application. **(May 2015)**

Ans. Remote and distributed data processing applications can be controlled in many ways. Some of these are given as follows:

- Remote access to computer and data files through the network should be implemented.
- Having a terminal lock can assure physical security to some extent.
- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
- In order to prevent the unauthorized users' access to the system, there should be proper control mechanisms over system documentation and manuals.
- Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
- When replicated copies of files exist at multiple locations, it must be ensured that all are identical copies that contain the same information and checks are also done to ensure that duplicate data does not exist.

Q11. Do you consider Corrective Controls are a part of Internal Controls? Describe the characteristics of Corrective Controls. **(May 2015)**

Ans. Yes, we consider Corrective Controls to be a part of Internal Controls. Corrective controls are designed to reduce the impact or correct an error once it has been detected. Contingency planning, Backup procedure, Rerun procedures, and Investigate budget variance and report violations are some of the examples of corrective controls.

The main characteristics of the corrective controls are as follows:

- Minimizing the impact of the threat;
- Identifying the cause of the problem;
- Providing remedy to the problems discovered by detective controls;
- Getting feedback from preventive and detective controls;
- Correcting error arising from a problem; and
- Modifying the processing systems to minimize future occurrences of the incidents

Q12. Explain Data integrity. What are the major data integrity policies? **(Nov 2014, Nov 2010)**

Ans. 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 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.

Q13. Discuss some of the critical controls required in a. computerized environment. **(Nov 2014)**

Ans. 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.

Q14. 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. **(Nov 2014)**

Ans. **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.

Q15. As an IS auditor, what are the output controls required to be reviewed with respect to application controls? OR 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.

(Nov 2014, May 2013)

Ans. 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.

As an IS Auditor, various Output Controls required to be reviewed with respect to Application Controls which are enforced for confidentiality, integrity and consistency of output 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.

Q16. Write a short note on Operating System Security. **(Nov 2014)**

Ans. **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.

Q17. Describe the various threats to the computerized environment due to cyber crimes. **(May 2014, Nov 2012)**

Ans. 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.

Q18. Explain the various financial control techniques used in information system control. **(May 2014)**

Ans. 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.

Q19. Write a short note on Information System (IS) security objective. **(May 2014)**

Ans. **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.

Q20. Describe any five major types of information security policy which company must maintain to meet the security objectives. **(Nov 2013, Nov 2011)**

Ans. 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.

Q21. Explain, briefly, the six categories of controls classified on the basis of nature of IS resources. **(Nov 2013)**

Ans. 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.

Q22. Write a short note on Locks on Doors with respect to Physical Access Control. **(Nov 2011)**

Ans. **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.

Chapter 4: Business Continuity Planning and Disaster Recovery Planning

Q1. List out the major activities to be carried out in the implementation of a Business Continuity Plan. **(May 2017)**

Ans. In the implementation of a Business Continuity Plan (BCP), the major activities that should be carried out include the following:

- Defining the scope and context;
- Defining roles and responsibilities;
- Engaging and involving all stakeholders;
- Testing of program on regular basis;
- Maintaining the currency and appropriateness of Business Continuity Program;
- Reviewing, reworking and updating the Business Continuity Capability, Risk Assessments (RA) and Business Impact Analysis (BIAs);
- Managing costs and benefits associated; and
- Convert policies and strategies into action.

Q2. What are the major documents that should be mandatorily part of any Business Continuity Management system? **(May 2017)**

Ans. The following documents (representative only) are classified as being part of the Business Continuity Management System:

- The Business Continuity Policy;
- The Business Continuity Management System;
- The Business Impact Analysis report;
- The Risk Assessment report;
- The aims and objectives of each function;
- The activities undertaken by each function;
- The Business Continuity strategies;
- The overall and specific Incident Management Plans;
- The Business Continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training program.

Q3. In today's fiercely competitive business environment which allows for no downtime, a comprehensive Business Continuity Plan is of paramount importance. What are the various components of a BCM process? **(May 2017)**

Ans. The various components of Business Continuity Management (BCM) Process are as follows:

- **BCM – Process:** The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.
- **BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
- **BCM – Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services.
- **BCM – Development and Implementation Process:** Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
- **BCM – Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.
- **BCM – Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

Q4. Explain the maintenance tasks undertaken in the Development of BCP. **(Nov 2016)**

Ans. The maintenance tasks undertaken in development of Business Continuity Planning (BCP) are to:

- Determine the ownership and responsibility for maintaining the various Business Continuity Planning (BCP) strategies within the enterprise;
- Identify the BCP maintenance triggers to ensure that any organizational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date;
- Determine the maintenance regime to ensure the plan remains up-to-date;
- Determine the maintenance processes to update the plan; and
- Implement version control procedures to ensure that the plan is maintained up-to- date.

Q5. What competencies are necessary for personnel assigned specific management responsibilities within the system while developing BCM? **(Nov 2016)**

Ans. While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system are as follows:

- Actively listens to others, their ideas, views and opinions;
- Provides support in difficult or challenging circumstances;
- Responds constructively to difficult circumstances;
- Adapts leadership style appropriately to match the circumstances;
- Promotes a positive culture of health, safety and the environment;
- Recognizes and acknowledges the contribution of colleagues;
- Encourages the taking of calculated risks;
- Encourages and actively responds to new ideas;
- Consults and involves team members to resolve problems;
- Demonstrates personal integrity; and
- Challenges established ways of doing things to identify improvement opportunities.

Q6. Write a short note on Types/Techniques of Back –ups. **(Nov 2016, Nov 2014, Nov 2011)**

Ans. Various types of back-ups are 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. At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed.
- **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 is very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
- **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.
- **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.

Q7. Explain the five stages or components of the BCM process. **(May 2016)**

Ans. The stages or components of the BCM process are as follows:

- **Stage 1: BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
- **Stage 2: BCM – Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the

enterprise continues to provide those products and services. The selection of strategy will take into account the processes and technology already present within the enterprise.

- **Stage 3: BCM – Development and Implementation Process:** This deals with the development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
- **Stage 4: BCM – Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and identifies opportunities for improvement.
- **Stage 5: BCM – Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service

Q8. What are the steps to be taken by an IS auditor with respect to IT in the process of BCP/DRP audit? **(May 2016, May 2014)**

Ans. During a BCP/DRP Audit of Information Technology, IS auditor is expected to follow these steps:

- 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 plan for alternate means of data transmission if 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 weakness identified in the last test 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?

Q9. Explain the various plans that need to be designed for Business Continuity Management. OR Explain the components of Disaster Recovery Plan. **(Nov 2015, Nov 2011)**

Ans. There are various kinds of plans that need to be designed for Business Continuity Management (BCM) that include the following:

- **Emergency Plan:** The Emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g. major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an enterprise undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

- **Back-up Plan:** The Backup plan specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system. For example, it might be difficult to specify; exactly how an organization's mainframe facility will be recovered in the event of a fire. The backup plan needs continuous updating as changes occur. For example, as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly.
- **Recovery Plan:** The Recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specifics 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. Periodically, the recovery committee must review and practice executing their responsibilities so they are prepared in case a disaster occurs.
- **Test Plan:** The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plan or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted.

Q10. Write a short note on Third party site for backup and recovery. OR A company has decided to outsource a third party site for its alternate back-up and recovery process. What are the issues to be considered by the security administrator while drafting the contract? **(Nov 2015, May 2010)**

Ans. If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as -

- how soon the site will be made available subsequent to a disaster;
- the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- the priority to be given to concurrent users of the site in the event of a common disaster;
- the period during which the site can be used;
- the conditions under which the site can be used;
- the facilities and services the site provider agrees to make available; and
- What controls will be in place and working at the off-site facility?

Q11. What are the tasks you will undertake to ensure that BCM program is in place, while assessing BIA? **(May 2015)**

Ans. Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The tasks to be undertaken to ensure that BCM program is in place while assessing BIA are as follows:

- Assess the impacts that would occur if the activity was disrupted over a period of time;
- Identify the maximum time period after the start of a disruption within which the activity needs to be resumed;
- Identify critical business processes;

- Assess the minimum level at which the activity needs to be performed on its resumption;
- Identify the length of time within which normal levels of operation need to be resumed; and
- Identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

Q12. As an IS auditor, what are the key areas you would verify during review of BCM arrangements of an enterprise. OR While doing audit or self assessment of the BCM Program of an enterprise, briefly describe the matters to be verified. **(May 2015, Nov 2014)**

Ans. During review of BCM arrangements of an enterprise, an IS auditor 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 that have been 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.

Q13. Write short note on Back-up option sites for Alternate processing facility arrangements. **(May 2015, May 2011)**

Ans. Security administrators should consider the following Backup option sites for alternate processing facility arrangements:

- **Cold site:** A cold site has all the facilities needed to install a mainframe system- raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
- **Hot site:** All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain and are usually shared with other organisations that have hot-site needs.
- **Warm site:** A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install.
- **Reciprocal agreement:** Two or more organisations 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.

Q14. Explain the objectives of Business Continuity Management Policy briefly. **(Nov 2014)**

Ans. 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.

Q15. Discuss the methodology of developing a Business Continuity Plan. **(May 2014)**

Ans. 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 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 ongoing business planning and system development processes in order that the plan remains viable over time.

Q16. How an auditor will determine whether the disaster recovery plan was developed using a sound and robust methodology? Explain. **(Nov 2013, Nov 2012)**

Ans. An auditor may determine whether the disaster recovery plan was developed by using a sound and robust methodology by evaluating the following elements:

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

Q17. Write a short note on Goals of the Business Continuity Plan. **(Nov 2013, Nov 2012)**

Ans. **Goals of a Business Continuity Plan:** Major goals of a business continuity plan should be to:

- identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

Q18. Which aspects should be covered while drafting IS security policy for Business Continuity Planning? **(May 2013)**

Ans. The following are the major aspects, which should be covered while drafting IS Security Policy for Business Continuity Planning:

- A Business Continuity Plan (BCP) must be maintained, tested and updated if necessary. All staff must be made aware of it.
- A Business Continuity and Impact Assessment must be conducted annually.
- Suppliers of network services must be contractually obliged to provide a predetermined minimum service level.
- If subsidiaries, divisions, departments, and other organizational units wish to be supported by the management information systems department on a priority basis in the event of an emergency or a disaster, they must implement hardware, software, policies, and related procedures consistent with related standards.
- Computer operations management must establish and use a logical framework for segmenting information resources by recovery priority. This will in turn allow the most critical information resources to be recovered first. All departments must use the same framework when preparing information systems contingency plans.
- In addition, recovery priority of all the applications must also be defined by assessing the criticality of the applications. Further, a classification may also be done for application criticality.
- Management must prepare, periodically update, and regularly test emergency response plans and disaster recovery plans that will allow all critical computer systems to continue processing and be available in the event of an interruption or degradation of service and also in the event of a major loss, such as a flood, earthquake.

Q19. What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity. **(Nov 2010)**

Ans. 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.

Chapter 5: Acquisition, Development & Implementation of Information Systems

Q1. Maintaining the system is an important aspect of system development. What are the categories of system/software maintenance? **(May 2017, May 2016, May 2014)**

Ans. System Maintenance can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled Maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting 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 during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.
- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the 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 with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

Q2. Application programs are written, tested and documented to convert the design specifications into a functional system. Explain the characteristics that a good coded application program should have. **(Nov 2016, Nov 2012)**

Ans. Application programs are written, tested and documented to convert the design specifications into a functional system. A good coded application 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 subsequently 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 considering all possible inputs and outputs of a program in case of least likely situations.

- **Accuracy:** It refers not only to 'what program is supposed to do', but should also take care of 'what it should not do'. The second part becomes more challenging for quality control personnel and auditors.
- **Efficiency:** It refers to the performance per unit cost with respect to relevant parameters and it should not be unduly affected with the increase in input values.
- **Usability:** It refers to a user-friendly interface & easy-to-understand internal/external documentation.
- **Readability:** It refers to the ease of maintenance of program even in the absence of the program developer.

Q3. "A variety of tasks during the SDLC are performed by special teams/individuals." Define in brief the role(s) of – (i) Systems Analyst (ii) Programmer (iii) Database Administrators (iv) Domain Specialist (v) IS Auditor (vi) Quality Assurance. **(Nov 2016)**

Ans. A variety of tasks during the System Development Life Cycle (SDLC) are performed by special teams/individuals. The roles are as follows:

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

(ii) **Programmer:** Programmer is a mason of the software industry, who converts design into programs by coding using programming language. Apart from developing the application in a programming language, they also test the program for debugging activity to assure correctness and reliability.

(iii) **Database Administrators:** The data in a database environment must be maintained by a specialist in database administration to support the application program. The DBAs handle multiple projects; ensures the integrity and security of information stored in the database and helps the application development team in database performance issues. Inclusion of new data elements must be done only with the approval of the database administrator.

(iv) **Domain Specialist:** Whenever a project team must develop an application in a field that's new to them, they take the help of a domain specialist. For example, if a team undertakes application development in Insurance, about which they have little knowledge, they may seek the assistance of an Insurance expert at different stages. This makes it easier to anticipate or interpret user needs. A domain specialist need not have knowledge of software systems.

(v) **IS Auditor:** As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. S/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.

(vi) **Quality Assurance:** This team sets the standards for development, and checks compliance with these standards by project teams on a periodic basis. Any quality assurance person, who has participated in the development process, shall not be viewed as 'independent' to carry out quality audits.

Q4. Write a short note on Final Acceptance Testing. **(Nov 2016)**

Ans. **Final Acceptance Testing:** It is a type of System Testing under Systems Development Life Cycle (SDLC) which is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system satisfies the users.

The final acceptance testing has two major parts:

- **Quality Assurance Testing:** It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance policy, methodology and prescriptions.
- **User Acceptance Testing:** It ensures that the functional aspects expected by the users have been well addressed in the new system. Alpha Testing and beta Testing are two types of the user acceptance testing. Alpha Testing is the first stage often performed by the users within the organization by the developers to improve and ensure the quality / functionalities as per user satisfaction. Beta testing is the second stage generally performed by the external users after deployment of the system.

Q5. Discuss the factors to be considered to validate a vendor's proposal at the time of software acquisition. **(May 2016)**

Ans. The contracts and software licensing process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming. The following factors have to be considered to validate a vendors' proposal at the time of software acquisition:

- The Performance capability of each proposed System in Relation to its Costs;
- The Costs and Benefits of each proposed system;
- The Maintainability of each proposed system;
- The Compatibility of each proposed system with Existing Systems; and
- Vendor Support.

Q6. Describe the prototyping model of system development explaining the generic phases of this model. **(May 2016)**

Ans. The traditional approach to develop a system sometimes may take years to analyze, design and implement a system. More so, many a times we know a little about the system until and unless we go through its working phases, which are not available. In order to avoid such bottlenecks and overcome the issues, organizations are increasingly using prototyping techniques to develop smaller systems such as Decision Support System, Management Information System, 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 modifying/replicating/expanding or even replacing it by a full-scale and fully operational system. As users work with the prototype, they learn about the system criticalities and make suggestions about the ways to manage it. These suggestions are then incorporated to improve the prototype, which is also used and evaluated. 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.

The generic phases of Prototyping model of a system development are as follows:

♦ **Identify Information System Requirements:** In traditional approach, the system requirements are 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.

- **Develop the Initial Prototype:** The designers create an initial base model and give little or no consideration to internal controls, but instead emphasize system characteristics such 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.
- **Test and Revise:** After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment and 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 reevaluation. Thus iterative process of modification and reevaluation continues until the users are satisfied.
- **Obtain User Signoff of the Approved Prototype:** 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. Prototyping is not commonly used for developing traditional applications such as accounts receivable, accounts payable, payroll, or inventory management, where the inputs, processing, and outputs are well known and clearly defined.

Q7. Feasibility Study is an important aspect of System Development Life Cycle (SDLC). Explain the dimensions, which are evaluated for this study. **(May 2016)**

Ans. Feasibility Study is an important aspect of System Development Life Cycle (SDLC). The dimensions under which Feasibility Study of a system is evaluated are as follows:

- **Technical Feasibility:** Tries to get the answer of "Is the technology needed available?"
- **Financial Feasibility:** This checks "Is the solution viable financially?"
- **Economic Feasibility:** Deals with the question "Evaluation of the Return on Investment"
- **Schedule/Time Feasibility:** This handles "Can the system be delivered on time?"
- **Resources:** Deals with the concern on "Are human resources reluctant for the solution?"
- **Operational Feasibility:** Checks for the question "How will the solution work?"
- **Behavioral Feasibility:** Deals with "Is the solution going to bring any adverse effect on quality of work life?"
- **Legal Feasibility:** Answers the question "Is the solution valid in legal terms?"

Q8. You have been associated with a system analysis team. Describe the important factors that you will consider while designing user input forms. **(Nov 2015)**

Ans. The important factors that a system analysis team member will consider while designing user input forms are as follows:

- **Content:** This refers to the actual pieces of data to be gathered to produce the required output to be provided to users. The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. New documents for collecting such information may be designed.

- **Timeliness:** Timeliness refers to when users need outputs, which may be required on a regular, periodic basis - perhaps daily, weekly, monthly, at the of quarter or annually. Data needs to be 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.
- **Format:** Input format refers to the manner in which data are physically arranged. After the data contents and media requirements are determined, input formats are designed on the basis of few constraints like - the type and length of each data field as well as any other special characteristics (number decimal places etc.).
- **Media:** Input medium refers to the physical device used for input or storage. This includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives may include display workstations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.
- **Form:** Form refers to the way the information is inputted in the input form and the content is presented to users in various output forms - quantitative, non- quantitative, text, graphics, video and audio. Forms are pre-printed papers that require people to fill in responses in a standardized way. Forms elicit and capture information required by organizational members that often will be input to the computer. Through this process, forms often serve as source documents for the data entry personnel.
- **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 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.

Q9. Describe the categories of tests that a programmer typically performs on a program unit. OR Discuss the benefits and limitations of unit testing. **(Nov 2015, May 2015, Nov 2014, May 2010)**

Ans. **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, 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. 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.

Q11. Write a short note on SDLC. **(Nov 2015)**

Ans. **SDLC (System Development Life Cycle):** The System Development Life Cycle provides system designers and developers to follow a sequence of activities. It consists of a generic sequence of steps or phases in which each phase of the SDLC uses the results of the previous one. The SDLC is document driven, which means that a phase of the SDLC is not complete until the appropriate documentation or artifact is produced. Some of the advantages of this system are - Better planning and control by project managers; Compliance to prescribed standards ensuring better quality; Documentation that SDLC stresses on is an important measure of communication and control; and the phases that are important milestones and help the project manager and the user for review and signoff. The sequential phases of SDLC Cycle are as follows:

1. Preliminary investigation
2. Systems Requirements Analysis
3. Systems Design
4. Systems Acquisition
5. Systems Development
6. Systems Testing
7. Systems Implementation; and
8. Post Implementation Review and Maintenance

Q12. Many-a-time organizations fail to achieve their system development objectives. Justify the statement giving reasons. **(May 2015)**

Ans. Many-a-time organizations fail to achieve their systems development objectives. Some of the most notable reasons for this are as follows:

(i) **User Related Issues:** It refers to those issues where user/customer is reckoned as the primary agent.
- **Shifting User Needs:** User requirements for IT are constantly changing and the development team faces the challenge of developing systems whose very purpose might change since the development process began.
- **Resistance to Change:** People have a natural tendency to resist change.
- **Lack of User Participation:** Users must participate in the development efforts to define their requirements, feel ownership for project success, and work to resolve development problems.
- **Inadequate Testing and User Training:** New systems must be tested before installation to determine that they operate correctly and users must be trained to effectively utilize the new system.

(ii) **Developer Related Issues:** It refers to the issues and challenges with regard to the developers.
- **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 often lack sufficient educational background and requisite state of the art skills.

(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.

- **Lack of Senior Management Support and Involvement:** Senior management must provide guidance to developers and users of information systems in terms of which development projects are important so that they act accordingly.
- **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 new technologies in practice. To obtain a required skill set in order to adapt new technologies becomes a major challenge for the organizations.

Q13. Define the Agile model of software development and, discuss its strengths. **(Nov 2014, Nov 2013)**

Ans. **Agile Model:** This is an organized set 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.

Some of the strengths of Agile Model identified by the experts and practitioners include the following:

- Agile methodology has the concept of an adaptive team, which enables 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 requirement of the customer has changed.
- Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.
- The documentation is crisp and to the point to save time.
- The end result is generally the high quality software in least possible time duration and satisfied customer.

Q14. Write a short note on Design of database. **(Nov 2014, May 2012)**

Ans. **Design of Database:** Design of the database involves determining its scope ranging from local to global structure. The scope is decided on the basis of interdependence among organizational units. The design of the database involves following four major activities.

- **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.

Q15. Describe the contents of System Requirement Specification (SRS) for a typical software development. **(May 2014, Nov 2011)**

Ans. 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.

Q16. Explain the role of auditor in information processing system design through SDLC. **(May 2014)**

Ans. 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.

Q17. Describe the strength, of waterfall approach to system development. **(May 2014)**

Ans. 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.

Q18. What issues you would like to raise during the technical feasibility of new proposed system? **(Nov 2013)**

Ans. 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?

Q19. Suggest the controls that need to be in place at the time of application software acquisition or selection process. **(Nov 2013)**

Ans. The following are the major controls that are required to be in place at the time of application software acquisition or selection process:

- Information and system requirements are needed to meet the business and system goals, system processes to be accomplished, and the deliverables and expectations for the system. The techniques are interviews, deriving requirements from existing systems, identifying characteristics from related system, and discovering them from a prototype or pilot system.
- A feasibility analysis should be done to define the constraints or limitations for each alternative system from technical as well as business perspective. It should also include economic, technical, operational, schedule, legal or contractual, and political feasibility of the system within the organization scope.
- A detailed Request for Proposal (RFP) document needs to specify the acceptable requirements (functional, technical, and contractual) as well as the evaluation criteria used in the vendor selection process. The selection criteria should prevent any misunderstanding or misinterpretation.
- While identifying various alternatives, software acquisition involves the critical task of vendor evaluation. The vendor evaluation process considers the following:
  - Stability of the supplier company,
  - Volatility of system upgrades,
  - Existing customer base,
  - Supplier's ability to provide support,
  - Cost-benefits of the hardware/software in support of the supplier application, and
  - Customized modifications of the application software.

Q20. Write a short note on Types of System Testing. **(Nov 2013)**

Ans. **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.

Q21. What do you mean by system requirement analysis? List the activities to be performed during the phase of System Requirement Analysis. **(May 2013, May 2011)**

Ans. 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 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;
- 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.

Q22. What is the goal of a prototype model approach of software development? Enumerate the strength of this model. **(May 2013)**

Ans. 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.

Q23. What activities are involved in system conversion? Explain them briefly. **(May 2013)**

Ans. Conversion includes all those activities, which must be completed to successfully convert from the previous system to the new information system. These are given as follows:

- **Procedure conversion:** Operating procedures should be completely documented for the new system that applies to both computer-operations and functional area operations. Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures, output, and internal control 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.
- **File conversion:** Since large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. In order to the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate control, such as record counts and control totals, should be required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back up. This is necessary in case the files must be reconstructed from scratch after a "bug'' is discovered later in the conversion routine.
- **System conversion:** After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. All transactions initiated after this time are processed on the new system. Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems.
- **Scheduling personnel and equipment:** Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager. As users become more familiar with the new system, the job becomes more routine. Schedules should be set up by the system

manager in conjunction with departmental managers of operational units serviced by the equipment.

- **Alternative plans in case of equipment failure:** Alternative processing plans must be implemented in case of equipment failure. Priorities must be given to those jobs, which are critical to an organization, such as billing, payroll, and inventory. Critical jobs can be performed manually until the equipment is set right.

Q24. State the advantages of SDLC from the perspective of the IS Audit. **(Nov 2012, Nov 2010)**

Ans. 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.

Q25. What are the activities to be undertaken during the Post Implementation Review? **(Nov 2012)**

Ans. 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.

Q26. Write a short note on Information System Maintenance. **(Nov 2011)**

Ans. **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.

Q27. Discus in brief the various functional areas to be studied by a system analyst for a detailed investigation of the present system. **(Nov 2011, May 2011)**

Ans. 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

Q28. When the existing information system is to be converted into a new system, what are the activities involved in the conversion process? **(Nov 2010)**

Ans. 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.

Q29. 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? **(Nov 2010)**

Ans. 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.

Q30. Write a short note on Regression Testing. **(Nov 2010)**

Ans. **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.

Q31. What are the two primary methods through which the analyst would have collected the data? **(May 2010)**

Ans. 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.

Q32. Write a short note on Data Dictionary. **(May 2010)**

Ans. **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.

Chapter 6: Auditing of Information Systems

Q1. Explain the major aspects to be looked into by an IS Auditor? **(May 2017)**

Ans. The major aspects that an Information Systems (IS) Auditor must consider while implementing an MIS are as follows:

An auditor must–

- ♦ Assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored;
- ♦ Ensure 'what project control standards are to be complied with' & determining the extent to which compliance is being achieved;
- ♦ Examine system documentation such as functional specifications to arrive at an opinion on controls;
- ♦ Provide a list of the standard controls, over operational concerns such as response time, CPU usage, and random access space availability that he/she can use as an assessment criteria;
- ♦ Review Feasibility Study Report and different work products of the Feasibility study phase;
- ♦ Include technical experts to seek their opinion on the technical aspects of development of MIS;
- ♦ Give control objectives, directives and in general, validate the opinion expressed by technical experts;
- ♦ Review some of the control considerations like –
    - o Documented policy and procedures;
    - o Established Project team with all infrastructure and facilities;
    - o Developers/ IT managers are trained on the procedures;
    - o Appropriate approvals are being taken at identified mile-stones;
    - o Development is carried over as per standards, functional specifications;
    - o Separate test environment for development/ test/ production / test plans;
    - o Design norms and naming conventions are as per standards and are adhered to;
    - o Business owners testing and approval before system going live; Version control on programs;
    - o Source Code is properly secured;
    - o Adequate audit trails are provided in system; and
    - o Appropriateness of methodologies selected.
- ♦ Determine whether the system adequately meets earlier identified business requirements and needs post -implementation review.
- ♦ Determine if the expected benefits of the new system are realized and whether users are satisfied with the new system.
- ♦ Review which of the phases till implementation of MIS have not met desired objectives and whether any corrective actions were taken in post implementation review.

Q2. What should an IS Auditor evaluate while reviewing the adequacy of data security controls? **(May 2017)**

Ans. An Information Systems (IS) Auditor is responsible to evaluate the following while reviewing the adequacy of Data Security Controls:

- ♦ Who is responsible for the accuracy of the data?

- ♦ Who is permitted to update data?
- ♦ Who is permitted to read and use the data?
- ♦ Who is responsible for determining who can read and update the data?
- ♦ Who controls the security of the data?
- ♦ If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
- ♦ Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
- ♦ The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

Q3. What is the scope of IS Audit process? Explain the categories of IS Audit. **(May 2017, Nov 2012)**

Ans. 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.

Information Systems Audits has been categorized into following types:

(i) **Systems and Application:** It is an audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) **Information Processing Facilities:** This audit verifies that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

(iii) **Systems Development:** It is 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.

(iv) **Management of IT and Enterprise Architecture:** This audit verifies that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

(v) **Telecommunications, Intranets, and Extranets:** This is an audit to verify that controls are in place on the client (end point device), server, and on the network connecting the clients and servers.

Q4. IS Auditors review risks relating to IT systems and processes. Briefly discuss these risks. OR What are the functions of an IS auditor? **(May 2017, Nov 2015, Nov 2014)**

Ans. Information System Auditor often is the assessor of business risk, as it relates to the use of IT, to management. The auditor can check the technicalities well enough to understand the risk (not necessarily manage the technology) and make a sound assessment and present risk-oriented advice to management. Information Systems (IS) Auditors review risks relating to IT systems and processes; some of them are as follows:

♦ Inadequate information security controls. For example - missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.
♦ Inefficient use of resources, or poor governance. For example - 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 that includes phishing, hacking etc.

Q5. You are appointed as the IS Auditor of a large company with multiple locations across globe which are connected to a common platform. What are the steps you would take as part of your preliminary evaluation to fully comprehend the technology environment & control issues?

(May 2017, May 2015)

Ans. An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

♦ Analysis of business processes and level of automation;
♦ Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business;
♦ Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture;
♦ Studying network diagrams to understand physical and logical network connectivity;
♦ Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government;
♦ Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems; and
♦ Finally, Studying Information Technology policies, standards, guidelines and procedures.

Q6. Discuss in brief the major concerns to be addressed by an auditor in the different activities of the Programming Management Control Phase. **(May 2017)**

Ans. Some of the major concerns that an Auditor should address under different activities involved in Programming Management Control Phase are as under:

Phase	**Audit Trails**
Planning	•They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired. •They must evaluate how well the planning work is being undertaken.
Control	•They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. •They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample if past and current

	software development and acquisition projects carried out at different locations in the organization they are auditing.
Design	•Auditors should find out whether programmers use some type of systematic approach to design. •Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
Coding	Auditors should seek evidence – •On the level of care exercised by programming management in choosing a module implementation and integration strategy. •To determine whether programming management ensures that programmers follow structured programming conventions. •To check whether programmers employ automated facilities to assist them with their coding work.
Testing	•Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. •Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. •Auditors primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Maintenance	•Auditors need to ensure that effective and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. •Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

Q7. Write a short note on ISO 27001. **(May 2017)**

Ans. **ISO 27001:** ISO 27001 is the international best practice and certification standard for an Information Security Management System (ISMS). An ISMS is a systematic approach to manage Information security in an IS environment through which an organization identifies, analyzes and addresses its information security risks. It encompasses people, processes and IT Systems. ISO 27001 defines how to organise information security in any kind of organization, profit or non-profit, private or state-owned, small or large. This standard is the foundation of information security management that enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the organisation as defined policies and procedures.

The ISO 27001 can act as the extension of the current quality system to include security; provides an opportunity to identify and manage risks to key information and systems assets; provides confidence and assurance to trading partners and clients; acts as a marketing tool and allows an independent review and assurance to you on information security practices.

Q8. Define and elaborate categories of risks that affect a system and taken into consideration at the time of assessment or audit of information systems.
(Nov 2016)

Ans. Risks that affect a system and are taken into consideration at the time of assessment or audit of information systems can be differentiated as Inherent risk, Control Risk and Detection Risk. They are as follows:

- **Inherent Risk:** Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same. Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.
- **Control Risk:** Control risk is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.
- **Detection Risk:** Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

Q9. Discuss the ways audit trails can be used to support security objectives. **(Nov 2016, Nov 2011)**

Ans. Audit trails can be used to support security objectives in three ways:

- **Detecting Unauthorized Access to the system:** 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.
- **Facilitating the Reconstruction of 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 the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

- **Promoting 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.

Q10. Explain the key steps that can be followed for a risk-based approach to make an audit plan. **(Nov 2016)**

Ans. The key steps that can be followed for a risk-based approach to make an audit plan are as follows:

- Inventory the information systems in use in the organization and categorize them.
- Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
- Assess what risks affect these systems and the severity of the impact on the business.
- Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Q11. Proper assessment of the degree of risk is critical to the effectiveness of the audit. Discuss some of the critical factors to be considered by an IS Auditor as part of his/her preliminary review. **(Nov 2016)**

Ans. Proper assessment of the degree of risk is critical to the effectiveness of the audit. The following are some of the critical factors to be considered by an IS auditor as part of his/her preliminary review.

(i) **Knowledge of the Business:** Related aspects are General economic factors and industry conditions affecting the entity's business; Nature of Business, its products & services; General exposure to business; Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced; Level of competence of the Top management and IT Management, and finally, Set up and organization of IT department.

(ii) **Understanding the Technology:** This includes the process to gain a good understanding of the technology environment and related control issues. This could include consideration of analysis of business processes and level of automation; Role of IT in the success and survival of business; Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture; Studying network diagrams to understand physical and logical network connectivity; Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government; Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor and finally, Studying IT policies, standards, guidelines and procedures.

(iii) **Understanding Internal Control Systems:** For gaining understanding of Internal Controls emphasis is to be placed on compliance and substantive testing.

(iv) **Legal Considerations and Audit Standards:** The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work. The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit. The statutes or regulatory framework may impose stipulations about minimum set of control objectives to be achieved by the subject organization.

Sometimes, this may also include restrictions on the use of certain types of technologies e.g. freeware, shareware etc. The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non- compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

(v) **Risk Assessment and Materiality:** Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation. It implies the process of identifying the risk, assessing the risk, and recommending controls to reduce the risk to an acceptable level, considering both the probability and the impact of occurrence. Risk assessment allows the auditor to determine the scope of the audit and assess the level of audit risk and error risk (the risk of errors occurring in the area being audited).

Q12. ABC Ltd. is looking for a suitable IS auditor. Please send an introductory note to ABC Ltd. explaining your suitability by describing the skill set and competence you possess for the job other than your qualification. **(May 2016, Nov 2012)**

Ans. ABC Ltd. is looking for a suitable IS auditor. I hereby explain my suitability for the same, as I hereby announce that I possess the desired skill set that is generally expected to be with an IS auditor which includes the following:

- Sound knowledge of business operations, practices and compliance requirements;
- 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.
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems.

Q13. Describe how the application controls and their audit trail are categorised. OR Software Applications require interface between user and the business functions. Discuss User Controls describing various types of controls to be exercised to achieve system effectiveness and efficiency. **(May 2016, May 2015)**

Ans. The Application Controls are categorized as below:

- **Boundary Controls:** Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.
- **Input Controls:** These are responsible for bringing both the data and instructions in to the information system. Input Controls are validation and error detection of data input into the system.
- **Communication Controls:** These are responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.
- **Processing Controls:** These are responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.
- **Output Controls:** These are the controls 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.
- **Database Controls:** These are responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data- set of rules to perform operations on the data to help a manager to take decisions.

  The following two types of Audit Trail controls should exist in each application control:
  - An **Accounting Audit Trail** to maintain a record of events within the subsystem; and

- An **Operations Audit Trail** to maintain a record of the resource consumption associated with each event in the subsystem.

Q14. As an IS auditor of a company, you want to use SCARF technique for collecting some information, which you want to utilize, for discharging some of your functions. Briefly describe SCARF and the type of information that can be collected through the use of SCARF technique.

(May 2016, May 2013, May 2011)

Ans. **System Control Audit Review File (SCARF):** 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. Afterwards, auditors 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.

The information that can be collected through the use of System Control Audit Review File (SCARF) technique is as follows:

- **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.

Q15. The advent of computer has drastically transformed the mode of evidence collection by an auditor. Discuss the various issues involved in the performance of evidence collection and understanding the reliability of controls. OR Write a short note on Effect of Computers on Evidence Collection for audit. **(May 2016, May 2015, Nov 2014)**

Ans. The advent of computer has drastically transformed the mode of evidence collection by an auditor. The issues involved in the performance of evidence collection and understanding the reliability of controls 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 printed 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 (journalised) 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 organisations 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 who are the parties to the contract.

Q16. List and explain the advantages & disadvantages of continuous audit techniques.

(Nov 2015, May 2014, Nov 2011, May 2010)

Ans. 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 analysed 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 Integrated Test Facilities (ITFs), new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports

The following are some of the key disadvantages of the continuous auditing:

- Auditors should be able to obtain resources required from the organisation 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.

Q17. What are the factors influencing an organization towards controls and audit of computers? **(Nov 2015)**

Ans. The factors influencing an organization towards controls and audit of computers are as follows:

- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions require accurate data to make quality decision rules.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
- **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
- **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

Q18. As an IS auditor, what are the environmental controls verified by you, while conducting physical inspections? **(Nov 2015)**

Ans. Audit of environmental controls requires the Information Systems 'auditor to conduct physical inspections and observe practices. The Auditor should verify:

- The IPF (Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction;
- The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;
- The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
- Emergency procedures, evacuation plans and marking of fire exits. There should be half-yearly Fire drill to test the preparedness;
- Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors;
- Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment, and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power;
- Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc;
- Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time To Repair)are within acceptable levels; and
- Identify undesired activities such as smoking, consumption of eatables etc.

Q19. Write a short note on Objectives of IS Audit. **(Nov 2015)**

Ans. The major objectives of Information System Audit are as follows:

- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
- **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.
- **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
- **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

Q20. Different auditors go about IS auditing in different ways. Despite this, IS audit process can be categorized into broad categories. Discuss the statement explaining broad steps involved in the process. **(May 2015, May 2012)**

Ans. Information Systems (IS) audit process can broadly be categorized on the basis of audit of Systems and applications; Information processing facilities; Systems Development; IT management and enterprise architecture; and Telecommunications, Intranets and Extranets.

Different auditors go about IS auditing in different ways. However, broadly the steps involved in an IS audit process are as follows:

(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.

(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 evidences 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 that 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 analyzed.

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

Q21. Write a short note on Continuous and Intermittent Simulation (CIS). **(May 2014)**

Ans. **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.

Q22. 'Real time information system needs real time audit techniques like Integrated Test Facility (ITF) to provide continuous assurance.' Define and explain the ITF methodology. **(Nov 2013)**

Ans. **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.

Q23. Being an IS Auditor, what objectives can you set for the audit of systems under development and how can you achieve your objectives? **(Nov 2012)**

Ans. The audit of systems under development can have the following main objectives:

- to provide an opinion on the efficiency, effectiveness, and economy of the project management;
- to assess the extent to which the system being developed provides adequate audit trails and controls to ensure the integrity of data processed and stored; and
- to assess the controls being provided for the management of the system's operation.

For the first objective to achieve, an auditor will have to attend project and steering committee meetings and examine project control documentation and conducting interviews. This is to ensure

what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved.

For addressing the second objective, the auditor can examine system documentation, such as functional specifications, to arrive at an opinion on controls. The auditor's opinion will be based on the degree to which the system satisfies the general control objectives that any Information Technology system should meet. A list of such objectives should be provided to the auditee.

The same is true for the third objective, viz. system's operational controls. The auditor should provide a list of the standard controls over such operational concerns as response time, CPU usage, and random access space availability that the auditor has used as assessment criteria.

Chapter 7: Information Technology Regulatory Issues

Q1. Discuss "Authentication of Electronic Records" with reference to the IT Act.

(May 2017, Nov 2013, May 2011)

Ans. In IT Act, 2000, Section 3 defines “Authentication of Electronic Records”. This section provides the conditions subject to which an electronic record may be authenticated by means of affixing Digital Signature. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

Provisions of authentication of electronic records are given under Section 3 of Information Technology (Amendment) Act, 2008, which is given as follows:

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.

Q2. What is a "Protected System" under the IT Act? **(May 2017)**

Ans. In IT Act, 2000, Section 70 defines “Protected System” that is as follows:

Protected System

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system. [Section 70]

Q3. What is the information that an IS Auditor is expected to obtain at the audit location before proceeding with the IS Audit as per the provisions of IRDA? **(Nov 2016)**

Ans. Before proceeding with the IS Audit as per the provisions of IRDA (Insurance Regulatory and Development Authority of India), the IS auditor is expected to obtain the following information at the audit location:

- Location(s) from where Investment activity is conducted.
- IT Applications used to manage the Insurer's Investment Portfolio.
- Obtain the system layout of the IT and network infrastructure including: Server details, database details, type of network connectivity, firewalls other facilities/ utilities.
- Are systems and applications hosted at a central location or hosted at different office?
- Previous Audit reports and open issues / details of unresolved issues from Internal Audit, Statutory Audit, and IRDA Inspection / Audit.
- Internal circulars and guidelines of the Insurer.
- Standard Operating Procedures (SOP).
- List of new Products/funds introduced during the period under review along with IRDA approvals for the same.
- Scrip-wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.
- IRDA Correspondence files, circulars and notifications issued by IRDA.
- IT Security Policy.
- Business Continuity Plans.
- Network Security Reports pertaining to IT Assets.

Q4. What is ITIL? Elaborate "service designs' under ITIL. **(Nov 2016)**

Ans. **IT Infrastructure Library (ITIL):** The ITIL is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form known as ITILv3, ITIL describes procedures, tasks and checklists that are not organization- specific, used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

- **Service Design:** Service Design is one of the five volumes in ITIL framework that translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings. It further includes design principles and methods for converting strategic objectives into portfolios of services and service assets.
- **Service Catalogue Management:** Service Catalogue management maintains and produces the Service Catalogue and ensures that it contains accurate details, dependencies and interfaces of all

services made available to customers. Service Catalogue information includes ordering and requesting processes, prices, deliverables and contract points.

- **Service Level Management:** Service-level management provides for continual identification, monitoring and review of the levels of IT services specified in the Service-Level Agreements (SLAs). Service-Level Management is the primary interface with the customer and is responsible for ensuring that the agreed IT services are delivered when and where they are supposed to be; liaising with availability management, capacity management, incident management and problem management.
- **Availability Management:** Availability management targets allow organizations to sustain the IT service-availability to support the business at a justifiable cost. The high-level activities comprise of realizing availability requirements, compiling availability plan, monitoring availability and maintenance obligations. Availability management addresses many IT component abilities like reliability, maintainability, serviceability, resilience and security to perform at an agreed level over a period of time.
- **Capacity Management:** Capacity management supports the optimum and cost- effective provision of IT services by helping organizations match their IT resources to business demands. The high-level activities include application sizing; workload management; demand management; modeling; capacity planning; resource management and performance management.
- **IT Service Continuity Management:** IT Service Continuity Management (ITSCM) covers processes by which plans are put in place & managed to ensure that IT services can recover & continue even after a serious incident occurs.
- **Information Security Management:** A basic goal of security management is to ensure adequate information security, which in turn, is to protect information assets against risks, and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their confidentiality, integrity and availability, along with related properties or goals such as authenticity, accountability, non-repudiation and reliability.
- **Supplier Management:** The purpose of Supplier Management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, Service Level Agreements and Service Level Requirements. Supplier Management oversees process of identification of business needs, evaluation of suppliers, establishing contracts, their categorization, management and termination.

Q5. Write a short note on Indian Computer Emergency Response Team. **(Nov 2016)**

Ans. **Indian Computer Emergency Response Team (CERT – In):** The Section 70B of IT (Amendment) Act, 2008 provides guidelines on how Indian Computer Emergency Response Team serves as national agency for incident response. The team shall serve as the national agency for performing the following functions in Cyber Security, which are as follows:

- Collection, analysis and dissemination of information on cyber incidents;
- Forecast and alerts of cyber security incidents;
- Emergency measures for handling cyber security incidents;
- Coordination of cyber incidents response activities;

- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
- Such other functions relating to cyber security as may be prescribed.

Q6. What are the suggested system controls that should be covered under IS audit as per the requirement of the Reserve Bank of India? **(May 2016)**

Ans. The System Controls that should be covered under the Information Systems' audit as per the requirement of the Reserve Bank of India (RBI) are as follows:

- Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming/design. System person would only make modifications/improvements to programs and the operating persons would only use such programs without having the right to make any modifications.
- Contingency plans/procedures in case of failure of system should be introduced/ tested at periodic intervals. EDP auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.
- An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements.
- In order to bring about uniformity of software used by various branches/offices, there should be a formal method of incorporating change in standard software and it should be approved by senior management. Inspection and Audit Department should verify such changes from the view-point of control and for its implementation in other branches in order to maintain uniformity.
- Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.
- There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.
- With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the banks Internal Audit including IS Audit to validate the approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Charter/Audit Policy.

Q7. ABC Ltd. is not aware of the importance and requirement relating to 'Retention of Electronic Records' as per IT Act, 2008. Please enlighten them on this.
(May 2016, May 2014, May 2012, May 2011, May 2010)

Ans. "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.

As per IT Act, 2008, "Section 7 deals with Retention of Electronic Records". The Section provides that -

(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, if -

(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:

PROVIDED that 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.

Q8. As per IT (Amended) Act, 2008, describe the power to make the rules by Central Government in respect of Electronic Signature. **(Nov 2015, May 2012)**

Ans. Section 10 of IT (Amendment) Act, 2008, describes the Power to make rules by Central Government in respect of Electronic Signature. The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of Electronic Signature;

(b) the manner and format in which the Electronic Signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing 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.

Q9. Describe the service strategy of ITIL, framework. **(Nov 2015)**

Ans. **Service Strategy:** The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service-provider investments in services. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers. The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset.

The components of service strategies are as follows:

- IT Service Generation
- Service Portfolio Management
- Financial Management
- Demand Management
- Business Relationship Management

Q10. The manner of selecting auditors builds confidence among various stakeholders. Describe SEBI norms for selecting an auditor. **(May 2015)**

Ans. The SEBI norms for Auditor Selection are as follows:

- Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the major Areas mentioned under SEBI's Audit Terms of Reference (TOR).
- The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (ISC)².
- The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like COBIT.
- The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. He should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
- The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

Q11. Mr. A has hacked into Defence Information Systems with an intention to steal classified information that threatens the security and sovereignty of India. He has used the services of a local cafe, 'CyberNet' for this purpose. The owner of 'CyberNet' tries to stop Mr. A but is threatened by Mr. A. Hence the owner of 'CyberNet' does not disclose A's activities to anyone. Mr. A is caught by the Vigilance Officers of the department.

(i) Is Mr. A punishable for his activities?

(ii) Is the intermediary, 'CyberNet' liable?

Please discuss the liabilities enunciated under the relevant sections of the Information Technology Act, 2000 in the above two cases. **(May 2015)**

Ans.

(i) Yes, Mr. A is punishable for his activities under the Section 66F.

[Section 66F(1)(B)] Punishment for cyber terrorism

Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Considering the facts provided in the case where Mr. A hacked into Defense Information System with an intention to steal classified information threatening the security and sovereignty of India, Mr. A is punishable for his activities.

(ii) Yes, Intermediary 'CyberNet' is liable under the Section 79.

[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.

Thus, according to Section 79(2)(c); the Intermediary 'CyberNet' failed to observe due diligence in discharging his duties and also the other guidelines as prescribed by the Central Government. So, Intermediary 'CyberNet' is liable.

Q12. ABC Ltd. is a security market intermediary, providing depository services. Briefly explain the relevant requirements with respect to annual systems audit mandated by SEBI in this regard. **(Nov 2014)**

Ans. SEBI (Securities and Exchange Board of India) mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.

- The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.
- Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.
- Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.
- The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report.
- Audit has to be conducted and the Audit report be submitted to the Auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement. The report should also take previous audit reports in consideration and cover any open items therein.

- The Auditee management provides their comment about the Non-Conformities (NCs) and observations. For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI. The auditor should indicate if a follow-on audit is required to review the status of NCs. The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit.

Q13. Discuss briefly, the four phases of Information Security Management System (ISMS) prescribed by ISO 27001. **(Nov 2014)**

Ans. 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.

Q14. 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. **(May 2014)**

Ans. 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.

Q15. 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. **(May 2013)**

Ans. 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.

Q16. Explain the objectives and scope of the Information Technology Act 2000. **(May 2012)**

Ans. 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.

Q17. 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. **(May 2010)**

Ans.

(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.

Chapter 8: Emerging Technologies

Q1. The Cloud Computing Architecture comprises of two parts. Briefly describe these two parts.

(May 2017)

Ans. A Cloud computing architecture consists of two parts - a **Front End** and a **Back End** that connect to each other through a network, usually the Internet. A central server is established to be used for administering the whole system.

- **Front End Architecture:** The front end of the cloud computing system is the side - the computer user sees and interacts through and comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.
- **Back End Architecture:** Back end is the "cloud" section of the system and refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment.

Q2. Write short notes on following:
(a) Cloud vs. Grid Computing
(b) Community Cloud **(May 2017)**

Ans. (a) Some pertinent differences between Grid Computing and Cloud Computing are as follows:

Grid Computing	**Cloud Computing**
Grid Computing enables heterogeneous resources of computers to work cooperatively and collaboratively to solve a scientific problem.	Cloud computing provides the facility to access shared resources and common infrastructure offering services on demand over the network to perform operations that meet changing business needs.
While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit.	While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
A computational grid focuses on computationally intensive operations.	Cloud computing offers two types of instances: standard and high-CPU.

(b) **Community Cloud:** In Cloud Computing, the Community Cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some

combination of them, and it may exist on or off premises. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.
Community Cloud supports Collaborative and Distributive Maintenance, Partial Security, cost Effectiveness, collaborative work on the cloud, sharing of responsibilities among the organizations. The limitation of the community cloud is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud. It is not suitable in the cases where there is no collaboration.

Q3. What are the limitations of mobile computing? **(Nov 2016)**

Ans. Limitations of Mobile Computing are as follows:

- **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and Enhanced Data for GSM (Global System for Mobile Communication) Evolution (EDGE), and more recently 3G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.
- **Security Standards:** When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards. One can easily attack the VPN through a huge number of networks interconnected through the line.
- **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life. Mobile computing should also look into Greener IT in such a way that it saves the power or increases the battery life.
- **Transmission interferences:** Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.
- **Potential health hazards:** People who use mobile devices while driving is often distracted from driving are thus assumed to be more likely involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.
- **Human interface with device:** Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

Q4. Write short notes on the following:

(a) Major Components of WEB 3.0

(b) Advantages of BYOD **(Nov 2016)**

Ans. (a) The two major components of Web 3.0 are as follows:

(i) **Semantic Web:** This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines can take contextual decisions on their own by finding, combining and acting upon relevant information on the web.

(ii) **Web Services:** It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr in order to search for images.

To conclude, Web 3.0 helps to achieve a more connected open and intelligent web applications using the concepts of natural language processing machine learning, machine reasoning and autonomous agents.

(b) Advantages of Bring Your Own Device (BYOD) are as follows:

- **Happy Employees:** Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise he would be carrying his personal as well as organization provided devices.
- **Lower IT budgets:** The employees could involve financial savings to the organization since employees would be using the devices they already possess, thus reducing the outlay of the organization in providing devices to them.
- **IT reduces support requirement:** IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.
- **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.
- **Increased employee efficiency:** The efficiency of employees is more when the employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.

Q5. Cloud Computing service providers offer their services on the lines of several fundamental models. Describe the various types of Cloud Computing models. **(May 2016)**

Ans. Cloud Computing service providers offer their services on the lines of several fundamental models. Various types of Cloud Computing Models are as follows:

- **Infrastructure as a Service (IaaS):** IaaS providers offer computers, more often virtual machines and other resources as service. It provides the infrastructure / storage required to host the services ourselves i.e. makes us the system administrator and manage hardware/storage, network and computing resources. In order to deploy their applications, cloud clients install operating-system images and their application software on the cloud infrastructure. Examples of IaaS providers include: Amazon EC2, Azure Services Platform, Dyn DNS, Google Compute Engine, HP Cloud etc.
- **Platform as a Service (PaaS):** Cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of acquiring and managing the underlying hardware /software layers. In PaaS, one can make applications and software's on other's database. Thus, it gives us the platform to create, edit, run and manage the application programs we want. All the development tools are provided. Some of examples of PAAS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard etc.
- **Software as a Service (SaaS):** SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. For example, one can make his/her own word document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system- thus Google is provisioning software as a service.
- **Network as a Service (NaaS):** It is a category of cloud services where the capability provided to the cloud service user is to use network/transport connecting services. NaaS involves optimization of resource allocation by considering network and computing resources as a whole. Some of the examples are Virtual Private Network, Mobile Network Virtualization etc.
- **Communication as a Service (CaaS):** CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is

responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as- needed basis. This approach eliminates the large capital investments. Examples are Voice over IP (VolP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.

Q6. Describe the major components of Web 2.0 for social networks. **(May 2016)**

Ans. Major components that have been considered in Web 2.0 include the following:

- **Communities:** These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are a number of tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.
- **Blogging:** Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.
- **Wikis:** A Wiki is a set of co-related pages on a particular subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.
- **Folksonomy:** Web 2.0 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.
- **File Sharing/Podcasting:** This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.
- **Mashups:** This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps in order to find the exact information of a cell phone device from the internet, just by entering the cell number.

Q7. Describe the various benefits of Mobile Computing. **(May 2016)**

Ans. The benefits of Mobile Computing are as follows:

- Mobile computing is a versatile and strategic technology that increases information quality and accessibility, enhances operational efficiency, and improves management effectiveness.
- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledgebase at the job location.
- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

Q8. If the employees of a company are allowed to use personal devices such as laptop, smart-phones, tablets etc. to connect and access the data, what could be the security risks involved? Classify and elaborate such risks. OR Explain emerging BYOD threats. **(Nov 2015)**

Ans. The policy under which the employees of the company are allowed using Personal devices such as laptop, smart phones, tablets etc. to connect to the corporate network to access information and application is known as BYOD (Bring Your Own Device) policy. Under this, there will be certain amount of risk associated with the client's data, which can be classified into four areas given below:

- **Network Risks:** Under BYOD; when employees carry their own devices to workplace (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the company's network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need to be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.
- **Device Risks:** A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threat.
- **Application Risks:** When a majority of employees' phones and smart devices are connected to the corporate network that are not protected by security software, probability of concurrent mobile vulnerabilities increase. Organizations become unclear in deciding that 'who is responsible for device security – the organization or the user'.
- **Implementation Risks:** Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above mentioned threats.

Q9. What are the advantages of using cloud computing environment? **(Nov 2015)**

Ans. Major advantages of Cloud Computing environment are given below:

- **Cost Efficiency:** Cloud computing is probably the most cost efficient method to use, maintain and upgrade. The cloud is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.
- **Almost Unlimited Storage:** Storing information in the cloud gives us almost unlimited storage capacity. Hence, one does not need to worry about running out of storage space or increasing the current storage space availability.
- **Backup and Recovery:** Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.
- **Automatic Software Integration:** In the cloud, software integration is usually automatic wherein no additional efforts are taken to customize and integrate the applications as per our preferences and with great ease. Hence, one can handpick just those services and software applications that s/he thinks will best suit his/her particular enterprise.
- **Easy Access to Information:** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.
- **Quick Deployment:** Cloud computing gives us the advantage of quick deployment. Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes.

Q10. Management wants to know the major challenges in using Cloud Computing technology for running the new web application. Write any five challenges. **(May 2015)**

Ans. Major challenges in Cloud Computing Technology for running new Web application are as follows:

- **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality. With the use of encryption and physical isolation, data can be kept secret.
- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible.
- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure and natural calamities are all threats to availability.
- **Governance:** Due to the lack of control over the employees and services, there is problem relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization.
- **Trust:** Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.
- **Legal Issues and Compliance:** There are various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements.
- **Privacy:** The privacy issues are embedded in each phase of the Cloud design that includes both the legal compliance and trusting maturity.
- **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'.
- **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. Some of the Cloud providers use server/s from other service providers and thus there is a probability that the data is less secure and is more prone to the loss from external server.
- **Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The reliability and scalability of architecture is dependent on the design and implementation to support the overall framework.
- **Identity Management and Access control:** A robust federated identity management architecture and strategy internal in the organization provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.
- **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
- **Software Isolation:** Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture and evaluate the risks required for the organization.
- **Application Security:** Security issues relating to application security still apply when applications move to a cloud platform. Service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server.

Q11. Write a short note on Best practices of Green IT. **(May 2015)**

Ans. Best practices of Green IT are as follows:

- Involving stakeholders on campus yields policies and green IT initiatives more likely to be embraced by the campus community.
- Partnering takes advantage of existing efforts and ensures wider reach and more effective use of limited resources.

- Guidelines for using the best practices simplify adaption of green IT by campus users and encourage them to consider green computing practices the norm.
- On-going communication about and campus commitment to green IT best practices to produce notable results.

Q12. What are your recommendations for efficient use of computer and IT resources to achieve the objectives of 'Green Computing'? **(Nov 2014)**

Ans. 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.

Q13. Discuss some of the pertinent objectives in order to achieve the goals of Cloud Computing. **(Nov 2014)**

Ans. 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.