HAND NOTES ON ISCA

INFORMATION SYSTEMS CONTROL AND AUDIT

LATEST EDITION FOR CA FINAL MAY 2014 STUDENTS

Key Features:

- Full coverage in just 112 pages
- Question-Answer Format
- Covering past exams & RTPs

KAPIL SABHARWAL

Preface to the first edition

"Information Systems Control And Audit" is a very intricate subject which requires a great deal of patience while reading the subject for the first time. It is most often observe that the students give their lot of time to other subjects of CA final, although those subjects have equal importance and also the syllabus of those subjects is very vast yet this subject demands a good time from your total preparation time. It is also evident from the result of CA final exams of past attempts that the students who have even scored good marks in other subjects but unfortunately failed in this subject. The reason behind their failure was not the non-seriousness in this subject but in fact it becomes very difficult for a student to learn the typical wording of this subject. They even could not revise the syllabus on the day before their exam.

Therefore, in the light of the problems faced by the students, i thereby, have tried to compress the entire syllabus of this subject in ***just 112 pages*** covering almost entire syllabus and past year exam questions, RTPs and Practice Manual etc. For the convenience of easy reading, text is formatted with formatting features like bold, italics and underline. I would like to thanks "The Institute Of Chartered Accountants Of India" for providing student portal hosted on its website.

This book has been completed after the sincere and restless efforts put by spending the precious time. I would like to dedicate this book to **"RADHA SOAMI SATSANG BEAS"** for my internal support. I am also very thankful to my family for their continued support and motivation in writing this book.

I shall be very thankful to the readers for their valuable suggestions and feedback in order to improve this book in future as per their requirements.

"Wishing you all the best for your career"

KAPIL SABHARWAL
M.COM, CA (FINAL)
Jalandhar (Punjab)
Cakapil_1313@hotmail.com

INDEX

CHAPTER 1- INFORMATION SYSTEMS CONCEPTS

1. Define System

Ans. It is an orderly arrangement of a set of interrelated & interdependent elements that operate collectively to accomplish some common purpose or goal.

Example- Human body is a system consisting of several parts such as head,heart,hands,legs and so on.These parts are related by means of connecting networks of blood vessels & nerves and the system has a main goal of "Living".

2. Explain the various types of a System. **V.Imp.**

According to Elements **(i) Abstract System:** It is an orderly arrangement of inter-dependent ideas. **(ii) Physical System:** It is a set of Tangible elements which operate together to accomplish an objective.Eg. School System which consists of buildings,teachers, administrators & text books that function together to provide education to students	**According to Interactive Behavior** **(i) Open System:** It interacts freely with its environment by taking input & returning output.With change in environment,an open system also changes to match itself with the environment. **(ii) Closed System:** It neither interacts with the environment nor changes with the change in environment
According to Degree of Human Intervention **(i) Manual System:** In these systems, data collection, manipulation,maintenance & final reporting are carried out absolutely by human efforts. **(ii) Automated Systems:** In these systems,above mentioned tasks are carried out by using micro-processors.However,to some extent, system also depends on manual intervention.	**According to Working/Output - [RTP May 2014]** **(i) Deterministic System:** It operates in a predictable manner wherein the interaction among the parts is known with certainty. **Example**: If one has a description of the state of the system at a given point of time plus a description its operation,the next state of the system may be given exactly,without error. **(ii) Probabilistic system:** In such systems, output can be predicted with certain degree of error.**Example**: A set of instructions given to a human who may not follow them exactly.

3. What do you mean by System Entropy?How would you prevent it?

Ans. It refers to the process of system decaying or becoming disordered or disorganised.

Maintenance- Preventing or offsetting an increase in entropy requires inputs of matter and energy to repair,,replenish & maintain the system.This maintenance input is called **Negative Entropy**.

Open systems require more negative entropy for keeping a steady state of operations.

4. Explain briefly the General Model of a System.

Ans. Input i.e the data flowing into the system from outside.

Processing is the action of manipulating the input into a more useful form.

Output is the information flowing out of a system.

Storage is the means of holding info. for use at a later date.

Feedback occurs when the outcome has an influence on the input.

5. Define System Environment.

Components outside the system boundary are known as System environment.It is a collection of elements in which the system operates.These elements surround the system and interact with it.

6. Define System Boundary.

It is the limitation of system within which the system components work together.A system exists inside the boundary whereas the environment exists outside the boundary.

7. Distinguish between Sub-System & Supra-System.

Point of difference	Sub-System	Supra-System
Meaning	It is a set of inter-related components which constitute a part of a larger entity	The system immediate above a sub-system is known as Supra-system.
Process	These are analysed by the process of **Decomposition**	These are derived by the process of **Integration** of different sub-systems.
Example	Input,Control Unit,ALU etc are sub-systems of a computer system.	Sales order processing,customer service,promotion & publicity etc are the components of Marketing Supra-system.

8. Explain the Characteristics of Sub-systems.

Ans. (i) Decomposition: Since it is difficult to manage a complex system when considered as a whole.Therefore,for the sake of convenience & clarity,a system is divided into small systems.The process of dividing a system into small systems is called decomposition.The process of decomposition is continued until smallest sub-systems are of manageable size.

(ii) Simplification: The process of decomposition may lead to large no. of inter-connections,which may not be manageable.Thus, in order to reduce these large no. of inter-connections,a process of organising sub-systems is applied which is called Simplification.

(iii) Decoupling: If two sub-systems are connected tightly with each other then very close co-ordination is required between them for their operation.

Example: If the R/M is put directly into the production at the moment R/M arrives in the factory then R/M system is tightly coupled with the Production system.

9. Define System Stress & System Change.

System stress - A stress is a force transmitted by a system's supra-system that causes the system to change,so that the supra-system can achieve its own goals better.In trying to accommodate the stress,the system may impose stress on its sub-systems and so on.

System change - A system change because it undergoes stress.Sub-systems which do not adapt themselves to stress,tend to decay & terminate.

10. What is meant by Information?

Ans. The term "Data" and "Information" are often used interchangeably.However, the relation of Data to Information is that of R/M to F/P.A data processing system processes data to generate info. on which business decisions are based. Thus,the quality of info. determines the quality of action/decision.Therefore,Info. plays a vital role in the survival of a business.

11. Explain the Attributes/Characteristics of Info.

(i) Availability (iv) Reliability (vii) Purpose (x) Rate
(ii) Validity (v) Adequacy (viii) Value (xi) Frequency
(iii) Quality (vi) Transparency (ix) Mode & Format (xii)Decay

12. Distinguish b/w Internal & External Info.

Point of Difference	Internal Information	External Information
Source	This info is generated from the operations of the organisation at various functional areas.	It is collected from the external environment of the organisation.
Flow of Info.	The internal info gets processed & summarized from junior to top most level of mgt.	Data on such info is directly obtained by top level from external sources.
Purpose	Planning info related to external environment	Controlling info related to Internal environment.
Significance	It always pertains to the various operational units of the organisation.	It is considered to observe the effect of external info on he organizational performance.
Example	Production & Sales Report, Financial Statements	Govt Policies, New Laws & Regulations

13. Explain the Significance/Advantages of Info/Info system in Mgt process/Business Process. RTP May 2010; May 2010
Explain some of the important implications of Info system in business. RTP May 2013

Ans. (i) Info system helps take right decision at the right time.
(ii) Info systems help managers in effective decision-making.
(iii) Innovative ideas for solving critical problems may come out from good info system.
(iv) Knowledge gathered through info system may be utilised by managers in unusual situations.
(v) Based on well-designed info system, an organization may gain edge in the competitive environment.

14. Explain the factors on which info requirements of Managers/Executives depend.

Ans. The factors on which info requirements of managers/executives depend are as follows:
1.**Operational Function** (i) The grouping or clustering of several functional units on the basis of related activities into sub-systems is termed as Operational Function.
For Example Marketing is an Operational Function, as it is the clustering of several functional units like market research,advertising,sales analysis and so on.
(ii) The info requirement of different operational functions varies in content and in characteristics where the content of info depends upon the activities performed under an operational function.
For Example In case of Marketing Functions,the content of info may be about the consumer behavior,new product's impact in the market etc.

2.Type of Decision-Making:

Programmed /Structured Decisions	Non-Programmed/Unstructured Decisions
(i) Programmed decisions are made w.r.t familiar,routine & recurring problems where not much judgment & discretion is required but it is just a matter of identifying the problem & applying the rule. (ii) These decisions are made on problems & situations by reference to a pre-determined set of precedents,procedures,techniques and rules. (iii) As a problem/issue for decision-making emerges,the relevant pre-decided rule or procedure is applied,thus,simplifying the process of decision-making.	(i) These decisions are made on situations which are unusual & non-repetitive about which not much knowledge & info are available. (ii) These decisions are not made by reference to any pre-determined guidelines,standard operating procedures,precedents & rules But are made by application of managerial intelligence,Experience,Judgment & Vision to tackling the problems & situations. **For Example:** Problems such as sudden major change in Govt. Policies adversely affecting an industry.

3. Level of Management Activity:

(i) Strategic level or Top level: a) Decisions made at this level are based to handle critical problems for the survival & success of the organisation.
b) They have a vital impact on the direction & functioning of the organisation.
For Example-Decisions on plant location,introduction of new products etc.
(ii) Tactical level Or Middle level: a) This level lies in the middle of managerial hierarchy where managers plan,organise,lead & control the activities of other managers.
b) Decisions made at this level are known as tactical decisions or operational decisions.
c) These decisions are relatively short,specific & functional.
(iii) Operational level or Supervisory level: a) This level is the lowest level of managerial hierarchy wherein the managers co-ordinate the work of others who are not themselves managers.
b) They ensure that specific tasks are carried out effectively & efficiently.

15. Explain the Components of Computer Based Info System (CBIS).

Ans. CBIS is an info system where computer plays a major role.Such a system consists of following elements:

(i) Hardware: It refers to machinery including the computer itself which is often referred to as CPU & all of its support equipments like I/O devices,Storage devices & Communication devices.
(ii) Software: It refers to computer programs & the manuals that support them.Computer programs are machine readable instructions that direct the CBIS to produce useful info from the data.
(iii) Data: Data are the facts that are used by programs to produce useful info.
(iv) Procedures: These are the policies that govern the operation of a computer system.Procedures specify the actions that people should take in a step-by-step manner.
(v) People: People are probably the components of a CBIS that influence the success or failure of info systems.Users,Programmers,system Analysts & DBA are just some of the people associated with the CBIS.

16. Explain the Characteristics of CBIS. May 2011; RTP May 2013

Ans. (i) All systems work for some pre-determined objectives and the system is designed & developed accordingly.
(ii) A system has no. of sub-systems,if one sub-system fails,the whole system does not work.
(iii) No sub-system can work in isolation;it depends on other sub-systems for its inputs.
(iv) Diff. Sub-systems interact each other to achieve the goal of the system.
(v) The goal of individual sub-systems is of lower priority than the goal of the entire system.So,the work done by individual sub-systems is integrated to achieve the central goal of the system.

17. What are the major Areas of CBIS?

Area	Application/Use
Finance & Accounting	Typical sub-application areas under this sub-system are- Financial accounting,General Ledger,Accounts Receivable/Payable,Cash mgt,Treasury mgt,Investment mgt,Fund mgt & B/S.
Marketing & Sales	The Sales Deptt. may use an order processing system to keep status & track of orders,generate bills for the orders executed & delivered to the customer,strategies for rendering services during warranty period & beyond,analyzing the sales data by category such as- by Region,product,salesman or sales value.
Production or manufacturing	The system generates production schedules & schedules of material requirements,monitor the product quality,plans for replacement or overhauling the machinery and also helps in O/H cost control & waste control.
Inventory/Stores Mgt	The system is used to regulate the minimum & maximum level of stocks,raise alarms at danger level stock,identifying the imp. items in stock (ABC Analysis),identifying most frequently moving items (XYZ Analysis) etc.
Human Resource Mgt	HRM system achieves the goals like less disputes,right utilization of manpower & quiet environment in functional area.An HRM system may have Modules like - Personnel Administration,Recruitment Mgt,Travel Mgt,Benefit administration,Salary administration,promotion mgt.

18. Explain the Types of Info Systems at Different Levels.

Ans. Mgt at diff. Levels take decisions matching to their position or hierarchy in the organisation.So,diff. Types of info systems are designed & developed accordingly.Organisation can be considered as a pyramidal mgt structure with the corporate level managers at the top & operational managers at the bottom.Typical categories of data are manipulated at diff. Levels.
(i) **At the Lowest Level**,the routine office work like maintaining inward register & public interaction are mostly done. This level is managed by operational level managers. No decision-making process is carried out at this level.
(ii) **At the Middle Level of Mgt**,the decision-making process starts. Inputs from diff. Internal & external info sources are collected & processed for strategic decisions.
(iii) **At the Top Level**, the decisions are taken on the basis of the info passed from the middle level mgt.
Transaction processing system(TPS): Business activities involve transactions & these transactions are organised & manipulated to generate various info products for external use. TPS thus records & manipulates transaction data into usable info.

19. Explain the activities involved in Transaction Processing Systems (TPS).

Ans. (i) **Capturing data** to organise in files or databases
(ii) **Processing of files/databases** using application software.
(iii) **Generating info** in the form of reports.
(iv) **Processing of queries** from various quarters of the organisation.

20. Explain the Components of TPS.

Ans. (i) Inputs: Source documents such as invoice, slips etc are the physical evidence of inputs into the TPS. They serve several purposes like capturing data, providing a permanent file for future analysis etc.
(ii) Processing: This involves the use of journals & registers to provide a permanent & chronological record of inputs.
(iii) Storage: Ledgers 7 files provide storage of data on both manual & computerized systems.
(iv) Outputs: Any document generated in the system is output. Some documents are however both output & input. **For Example-** A customer invoice is an output from the order-entry application system & also an input document to the customer.

21. Explain the Features of TPS. RTP Nov 2013; Nov 2013

(i) Handling large volume of Data: Since transactions processing involves large volume of data & requires greater storage capacity. TPS handles large volume of data for processing & storage in it.
(ii) Automation of basic operations: TPS aims at automating the basic operations of an organisation & plays a critical role in the day-to-day functioning. TPS is an imp. source of up-to-date info regarding the operations in the enterprise because any failure in the TPS may disorder the functioning of an enterprise.
(iii) Benefits are easily measurable: Most of the benefits of TPS are tangible & easily measurable like TPS reduces the workload of the people associated with the operations & improves their efficiency. Therefore, Cost-Benefit Analysis regarding the desirability of TPS is easy to conduct.
(iv) Source of Input for other systems: TPS is the basic source of internal info for other systems like MIS,DSS,EIS etc.

22. Define MIS & also Explain the three Concepts of MIS.

Ans. **MIS** (i) It is an extension to TPS.
(ii) It uses the results produced by TPS but also uses other info.
(iii) It assists managers in decision-making & problem solving by providing them accurate, relevant & timely info in the form of Reports, Tables, Graphs & Charts.
(iv) MIS at the Top level is much more comprehensive.

Components of MIS

1.**Management:** Mgt comprises the processes or activities that describe what managers do in the operation of the organisation.a manager may be required to perform following activities in an organisation:
(i) Determination of organisational objectives.
(ii) Developing plans to achieve the objectives.
(iii) Exercising the adequate controls over the functions.
(iv) Monitoring the results.
(v) Securing & organizing the human & physical resources.
2.**Information:** It is the data that have been put into a meaningful & useful context. The info is considered to be of significance in a particular situation.
3.**System:** A system is defined as set of related components, activities, processes & human beings interacting together so as to accomplish some common objective.

23. Explain the Characteristics of MIS. **RTP May 2012 & Nov 2012; Nov 2013**

(i) Mgt oriented: Info provided by MIS should be Mgt oriented. But it should not necessarily be meant only for mgt at top level rather it should also meet the info needs of middle level & lower level mgt.
(ii) Mgt Directed: Mgt should direct the system's development efforts & should provide their time for system's designing, its review & should ensure that the implemented system meets the specifications as desired.
(iii) Common Database: DB should be so organized that it should allow access to other sub-systems & eliminates the necessity of duplication in data storage, updating, deletion & protection.
(iv) Common Data flows: It is possible due to use of common input, processing, output procedures & media. This eliminates duplication in data collections, simplifies operations & produces an efficient info system.
(v) Computerized: It helps in handling wide variety of applications by providing their info requirements quickly and provides accuracy & consistency in processing data.
(vi) Integrated: In a good MIS, all the functional & operational sub-systems are linked together into one unit which helps in generating more meaningful info.

24. Explain the Mis-Conceptions/Myths about MIS. **RTP Nov 2013**

1. **MIS is related only with computers:** This is not true because MIS can be Manual or Computerized. A computer is only a tool which helps in the timely & accurate info processing.
2. **More Data means More Info for managers:** This is a mis-conception. It is not the quantity of data but its relevance which is important to managers in the process of decision-making.
3. **Accuracy in Reporting is of Vital importance:** It is true only at operating levels. However,at the higher decision levels, great accuracy may not be required. **For Example:** For a decision on a new project proposal, top mgt is not interested in knowing the project cost in precise rupee terms. A project cost estimated at a fairly correct figure is sufficient.

25. What are the pre-requisites of an effective MIS? **Nov 2010; RTP May 2013**

Ans. 1. **Top Mgt Support:** The MIS to become effective, should receive full support of top mgt.
2. **Qualified system & mgt staff** i.e. it should be manned by qualified officers who are expert in the field of their work. There are two categories of officers:
(i) **Systems & Computer experts:** They should be capable of understanding mgt concepts to facilitate the understanding of problems faced by the concern and they should be clear about the process of decision-making & info requirements for planning & control functions.
(ii) **Mgt Experts:** They should also understand the concepts & operations of a computer so that they can place themselves in a comfortable position while working with the system technicians in designing etc of the info system.
3. **Database:** It can be defined as a "**Super-File"** which consolidates data records previously stored in many data files. Its main characteristic is that each subsystem utilizes the same data & info kept in the same file to satisfy its info needs. The maintenance of data in DB requires computer hardware, software & experienced computer professionals.
4. **Control & maintenance of MIS:** Control of MIS means the operations of the system as it was designed to operate.Mgt is closely related to control. There are times when the need for improvements to the system will be discovered.
5. **Evaluation of MIS:** It should take into account the following points:
(i) Examining whether, the enough flexibility exists in the system to cope with any expected or unexpected info requirement in future.
(ii) Ascertaining the views of users & the designers about the capabilities & deficiencies of the system.
(iii) Guiding the appropriate authority about the steps to be taken to maintain the effectiveness of MIS.

26. Explain the Constraints/problems/difficulties in operating a MIS. **RTP Nov 2012; May 2012**

(i) Non-Availability of Experts; (ii) Problem of selecting the sub-system of MIS to be installed & operated upon;
(iii) Due to varied objectives of business concerns, **the approach adopted by experts** for designing & implementing MIS **is a non-standardized one; and** (iv) Non-Availability of Co-operation from Staff

27. What are the effects of using Computer for MIS?

Ans. (i) Speed of processing & retrieval of data increases.

(ii) Scope of analysis widened
(iii) Complexity of system design & operation increased
(iv) Integrates the working of different sub-systems
(v) Increases the effectiveness of info system
(vi) More comprehensive info

28. What are the Limitations of MIS. Nov 2012, RTP May 2014

GIGO Principle: The quality of output depends on the quality of input & processes.

1. **Not a substitute for Effective mgt:** It can not replace managerial judgment in making decisions in different functional areas But it is merely a tool in the hands of executives for decision-making & problem solving.
2. **Less effective due to frequent changes in Top Mgt.**
3. **Less effective where culture of hoarding info prevails.**
4. **MIS may not have requisite flexibility** to quickly update itself with the changing needs of time, especially in fast changing & complex environment.
5. **MIS can not provide a Tailor-made info packages** suitable for every type of decision made by executives.
6. **It ignores non-quantitative factors** like morale & attitude of members of the organization.
7. **Less useful for making non-programmed decisions.**

29. What is a DSS? Explain the Characteristics of DSS. Nov 2008; RTP May 2012, RTP May 2014

Meaning of DSS: DSS are specific class of CBIS that supports business & organizational decision-making activities. In DSS, the focus is on helping decision makers to become more effective. DSS provides tools to managers to assist them in solving semi-structured & 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 enable them to generate the info required by them in making decisions.

Characteristics: (i) Semi-structured & Unstructured decisions: DSS is designed to support semi-structured & unstructured decision making. These are the decisions for which info obtained from the computer system is only a portion of total knowledge required to make the decisions.

Example of Unstructured Problem: A manager is selecting an accounting software for his company's use. This problem is unstructured because there is no listing of all the features that are desirable in accounting software for his particular co. furthermore; he will need to use his judgment to determine what features are important.

(ii) Flexibility to adapt changes: DSS designer understands that managers usually do not know in advance what info they need, Also, the info needs keep changing constantly. Thus, DSS provides tools to enable users to meet their own output needs.

(iii) Ease of learning & use: Since DSS are often built & operated by users rather than by computer professionals, the tools that accompany them should be relatively easy to learn & use.

30. Explain the various components of DSS.

Ans. 1. **The User:** The user is usually a manager with an unstructured or semi-structured problem to solve. Users, generally, do not require a computer background to use a DSS for solving problems but they require only a thorough understanding of the problem & factors to be considered in finding a solution. The user can be classified as under:

(i) **Manager:** They have basic computer knowledge & they desire the DSS to be very user-friendly.

(ii) **Staff specialist (Analysts):** They are more details oriented & willing to use complex system in their day to day work.

2. **Databases:** DSS include one or more databases that contain both routine & non-routine data from internal & external sources. DSS users may construct additional databases themselves. The database may also capture data from other subsystems such as marketing, production & personnel.
3. **Planning Languages:** Their types are as under:

(i) **General-Purpose planning languages**: These languages allow the users to perform many routine tasks & enable them to tackle a broad range of budgeting, forecasting & other worksheet-oriented problems.

(ii) **Special-Purpose planning languages:** These languages are more limited in what they can do but they do certain jobs better than the general-purpose planning languages.

4. **Model base:** It is the **"Brain" of DSS** because it performs data manipulations & computations with the data provided to it by the user & the database.

31. What are the levels in which Database is implemented in a DSS? Nov 2010

Ans. 1. **Physical Level:** It involves the implementation of the database on the hard disk.
2. **Logical Level:** It is designed by professional programmers who have complete knowledge of DBMS. It deals with:

(i) The Nature of data stored (ii) The Scheme of the data

(iii) The Storage, which is logically divided into various tables having rows & columns

(iv) The Techniques for defining relationships with indexes.

3. **External Level:** The Logical level defines Schema which is divided into smaller units known as Sub-Schema & given to the managers. Each Sub-schema contains all the relevant data needed by one manager.

32. DSS are widely used as a part of an organisation's accounting info system (AIS).Give example to support this statement.

Ans. A DSS is generally developed to solve specific problems. Which can be illustrated as below:

1. **Cost Accounting System:** The Cost Accounting applications help business in ascertaining cost, price,quotations,budgeting etc **For instance:** It helps health care Organisations to calculate product costs for individual procedures or services.
2. **Capital Budgeting System:** It provides tools (like **NPV,IRR** etc) to evaluate investments decisions. **Automan** is a DSS designed to support investment decisions in automated mfg technology. It allows decision makers to consider financial, non-financial, quantitative & qualitative factors in their decision-making process.
3. **Budget Variance Analysis System:** It assists in controlling costs & evaluating managerial performance. A Computerized DSS

can be used to generate monthly variance reports, to draw graphs and to view, analyze & comment on budget variances. It may also be used to create one & five year budget projections using the forecasting tools provided in the system.
3. **General DSS:** Here, the user needs to input data & answer questions about a specific problem domain to make use of this type of DSS.**Example - Expert Choice** is a program which supports a variety of problems requiring decisions. It analysis the judgments & presents the decision maker with the best alternative.

33. What are the Characteristics/Features of EIS? May 2011; Nov 2012

(i) EIS is a CBIS that serves the info needs of Top Executives.
(ii) It enables the users to extract summary data & model complex problems **without need to learn query languages**, statistical formulas or high computing skills.
(iii) It **provides rapid access** to timely info & direct access to mgt reports.
(iv) It is capable of **accessing both internal & external data.**
(v) It **provides extensive online analysis tool** like trend analysis,mkt conditions etc.
(vi) It can easily be given a DSS support for decision making.

34. Who is an Executive? What is the Role of Executive in Decision-Making?

Ans. An Executive is a manager at/near the top level who exerts a strong influence on the course taken by the firm. Most Executive decisions fall into following three categories:
1. **Strategic Planning:** It involves determining the general, long-range direction of the organization. The CEO is ultimately responsible for the development of strategic plans.
2. **Tactical Planning:** It refers to how, when, where & what issues involved with carrying out the strategic plan. Although, the executives do not normally concerned with the tactical details but still they worry about the general tactics.
3. **Fire Fighting:** Major problems require attention of managers at executive level.

Example- If a company is involved in a big lawsuit that threatens its financial solvency, an executive must get involved.
In addition to planning & fire-fighting, executive mgt also needs to exert some general control over the organization.

35. Successful Executives may take decisions relying more on intuition than on any quantitative analytical decision technique. Mention five Characteristics of the types of info that are responsible for this phenomenon in Executive decision-making. May 2010

Ans. Often, executives make decisions based on a vision so as to make their companies successful. That is why; executives rely much more on their own intuition than on the sophisticated analytical skills. The intuitive character of executive decision-making is reflected in the types of info found most useful to executives.

Characteristics of Executive Decision-making:
1. **Lack of structure:** Many of the decisions made by the executives are relatively unstructured. These types of decisions are not as clear-cut as deciding how to debug a computer program.
2. **High degree of uncertainty:** Executives work in a decision area that is often characterized by a lack of precedent or where results are not precisely predictable from actions.
3. **Future Oriented:** Executives are responsible to make sure that the organization keeps pointed toward the future.

For Instance - How will future technologies affect what the company is currently doing? What will the govt do next? What products will consumers demand five years from now?
4. **Informal Source:** Executives rely much more on the informal source for important info.

For Example - Lunch with a colleague in another firm might reveal some important competitor strategies.
5. **Low level of detail:** Executives take decisions based on trends. This requires the executive to be more aware of the large overview than the tiny items.

36. In what ways an EIS differ from the traditional info system? May 2013

Basis of Difference	Traditional Info System	EIS
Info sources	Internal	More External less Internal
Level of Mgt	For Lower Staff	For Top or near Top Executives
Nature of info provided	Offline status reporting	Online tools & analysis
Drill down facility to go through details at successive	Not available	Available
Info Format	Tabular	Text with graphics
Nature of Interface	Computer-operator generated	User-friendly

37. Discuss the general guidelines to design the measures & indicators of an EIS. Nov 07; RTP May & Nov 2012 & Nov 2013

Ans. EIS measures must be:
(i) Easy to understand & collect.
(ii) Based on the balanced view of the organisation's objective.
(iii) Available to everyone in the organisation.
(iv) Developed to meet the changing needs of the organisation.
(v) Able to encourage mgt & staff

Performance Indicators:
(i) Must reflect everyone's contribution in a fair & consistent manner.
(ii) Should be independent as possible from variables outside the control of managers.
(iii) Must promote both team-work & friendly competition.

38. What are Expert systems? List the Properties which an application should possess to qualify for Expert System Development. May 2013

Meaning: (i) ES is a highly developed DSS that utilizes knowledge generally possessed by a Human Expert to solve the problem.
(ii) ES provide decision makers with the type of advice they would receive from a Human Expert.

Major properties that potential applications should possess to qualify for ES development are as follows:
1. Availability - One or more experts should be available who are capable of communicating how they go about solving the problems.
2. Complexity - ES provide solution to complex problems that require logical inference processing which would not be normally handled by conventional info processing.
3. Domain -The domain or subject area of the problem is relatively small & limited as compared to a well defined problem area.
4. Expertise - Solution to the problems provided by ES should be as it was provided by experts because only a few persons possess the knowledge, techniques & intuition required for solving the problems
5. Structure -The solution process of ES must be able to cope with ill-structured, uncertain, missing & conflicting data.

39. Write short notes on business applications of Expert Systems for Mgt Support Systems. May 2011; RTP May 2012

Area	Applications/Examples
Accounting & Finance	ES provides advices on issues like Tax computation, Investment decisions, Credit Authorization decisions etc.
Marketing	It provides establishing Sales-Quotas, responding to Customer-Inquiries etc
Manufacturing	It assists Product designing, analyzing quality, selecting Transportation routes etc.
Personnel	It helps in assessing applicant's qualifications, filling out forms etc.
General Business	It assists in acquisition strategies, educating trainees, evaluating performance etc

40. Why is there need for Expert Systems?

Ans. (i) Expert labour is expensive & scarce.
(ii) Humans can handle only a few factors at a time.

41. List the Benefits of Expert Systems. Nov 2010, RTP May 2014

Ans. (i) It **Preserves knowledge** that might be lost through expert's retirement, death, resignation etc
(ii) It puts info into an active-form so it can be called as **Real-Life Expert.**
(iii) It **assists Novices** in thinking.
(iv) It is not subject to such **Human Limitations** such as fatigue, being too busy or being emotional.
(v) It can be effectively used as **Strategic Tool** in the areas of marketing,

42. Briefly explain the components of Expert Systems.

Knowledge Base	**(i)** It stores the **Rules, Data & Relationships** that are used to solve problems & contain specific facts about the expert area. **(ii)** With such a system, a **set of rules** must be developed to bridge the knowledge bases & to resolve the conflicts. **(iii)** The knowledge acquired from the expert has to be represented formally by using **Representation Techniques** like Production Rule Systems, a Structured Object & Predicate Calculus or Logic. **(iv)** The Power of a system depends on the **Depth & Breadth of Knowledge in the KB.**
Inference Engine	**(i)** It is the main processing element consisting of system of programs that **requests** data from the user, **manipulates** the KB & **provides** a decision to the user. **(ii)** It performs this task to deduce new facts which are then used to draw further conclusions. **(iii)** It is the active component of an expert system since it steers through knowledge & progresses the whole interaction.
Knowledge Acquisition Subsystem	**(i)** It is **a software component of an Expert System** that enables the Knowledge Engineer (KE) to build & refine an Expert System KB since the KE is a specialized System Analyst who is responsible for designing & maintaining the expert systems. **(ii)** KB development & maintenance can be done using **user-friendly software** that provides easy-to-operate menus & templates for entering rules, facts & relationship among facts.
User-Interface	**(i)** It is the method by which an expert system interacts with a user. These can br done through **Dialog Boxes, Command Prompts, Forms or Other Input Methods.** **(ii)** The ES prompts the user to supply info about the problem & the user types in the requested data. **(iii)** The data entered by the user are then examined by the inference engine & compared to the facts, rules & relationship in the KB that helps to reach a conclusion.

43. What are the types of Office Activities/Operations which can be automated? Nov 2010

Ans. (i) Document Capture i.e. preservation of documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc.
(ii) Document Creation i.e. preparation of documents, letters, dictation, editing of texts etc.
(iii) Receipt & Distribution i.e. handling & distribution of correspondence to designated recipients.
(iv) Filing, Search, Retrieval & Follow up i.e. filing, searching & follow up of documents.
(v) Calculations: These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations etc.
(vi) Recording utilization of Resources: This includes record keeping in respect to specific resources utilized by office personnel.

44. What are the benefits of OAS?

Ans. (i) Improved communication within & between Organizations
(ii) Reduced cycle time between preparation & receipt of messages at the recipient's end.
(iii) Reduced cost of communication (iv) Ensures accuracy of communication flows.

45. Write short notes on Text Processing Systems.

Meaning: Text processing systems are the most commonly used components of OAS. This is so because a large proportion of office communication takes place in writing using words of natural language.

Features of Text Processing Systems:

(i) Text processing systems automate the process of development of documents such as letters, reports; memos etc. They permit use of standard stored info to produce personalized documents. Such automation reduces keying effort & minimizes the chances of errors in the document.

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

46. Explain the Features of Electronic Document Mgt Systems (EDMS).

(i) EDMS assists in capturing the info contained in documents, stored for future reference & communicates to the users as & when required.

(ii) These systems are very useful in **Internal Communication** & in **Remote Access of Documents.** Therefore, the location of Executives becomes irrelevant for access to documents.

47. What are the various Components of Electronic Message Communication Systems?

(i) E-Mail (ii) Facsimile (FAX) (iii) Voice Mail

48. Explain the Features of E-Mail. **Nov 2012**

(i) Electronic Transmission **(ii)** Online Development & Editing **(iii)** Broadcasting & Re-routing
(iv) Integration with other systems **(v)** Portability **(vi)** Economical

49. Write short notes on FAX.

It is an electronic communication of images of documents over the telephone lines. The computer based FAX technology automates FAX communication & permits sharing of FAX facilities. It uses FAX servers to send & receive FAX messages.

50. Write short notes on Voice Mail.

This provides transmission of messages as digitized voice. The recipient of voice mail has to dial a voice mail service or access the e-mail box using the specified equipment & he can hear the spoken message in the voice of sender.

51. Write short notes on Teleconferencing & Video-conferencing systems.

Teleconferencing refers to electronic meetings that involve people at different physical locations. It may be of audio or video type with or without use of computer systems. Although, the computer based teleconferencing has the advantage of flexibility in terms of pre-recorded presentations & integration with other info systems.

Video-conferencing uses Display screens, video cameras & communication systems to link participants based at different locations. In this case, participants can hear & see each others.

Important Note: Please read the topic ERP from "CHAPTER 7".

Chapter 2 - System Development Life Cycle Methodology

1. What is System Development and Explain briefly the System development process?

Ans.Meaning of System Development: It refers to the process of examining a business situation with the intent of improving it through better procedures & methods.

System Development Process: Whenever mgt or system development personnel realize that a particular system needs improvement or they want to change the old info system with a new & improved info system,a process starts in the organisation which is known as system development process.It has two major Components:

1. **System Analysis:** Under this,the requirements for which the system is to be developed are thoroughly analysed by collecting various facts & figures in terms of features & problems of existing system.This analysis provides improvement over the existing system & meets all the specified requirements of new system.
2. **System Design:** It provides the design of all the required features of new system in the flowcharts & flow diagrams etc.It can be said as a **Blue Print of the system** to be developed.

2. What is System development methodology? Explain its features/characteristics.

Ans. Meaning: (i) A system development methodology is a formalized,standardized & documented set of activities used to manage a system development project.

(ii) It refers to the framework which is used to structure,plan & control the process of developing an info system.

The methodology is characterized by the following:

- **Division of Project:** The project is divided into a no. of identifiable processes which facilitates both project planning & project control.Each process has a starting & ending point and comprises of several activities,one or more deliverables & several mgt control points.
- **Deliverables:** Specific reports & other documentation called **Deliverables** must be produced periodically during system development so as to make development personnel accountable for the faithful execution of system development tasks.
- **Sign-offs:** Users,managers & auditors are required to participate in the project.Their participation generally provides approvals of development process & the system being developed,often called sign offs.
- **System Testing:** The system must be tested thoroughly prior to implementation to ensure that it meets users' needs.
- **Training Plan:** A training plan is developed for those who will operate & use the new system.
- **Controls:** Formal program change controls are established to preclude unauthorized changes to computer programs.
- **Post-implementation Review:** A PIR of all developed systems must be performed to assess the effectiveness & efficiency of the new system & of the development process.

3. Explain the SDLC framework.Also outline the general advantages of SDLC methodology.

Ans. Meaning: (i) This framework provides the system designers & developers to follow a sequence of activities that consists of a set of steps/phases in which each phase uses the result of previous phase.

(ii) The SDLC is **Document driven** which means that at crucial stages during the process,documentation (Also called artifact/Deliverables) is produced.

(iii) A phase is not complete until the deliverable is produced.

(iv) **Deliverable -** A deliverable may be a substantial written document,a software artifact,a system test plan or even a physical object

General Advantages of SDLC Methodology:

- Better planning & control by project managers.
- Compliance to prescribed standard ensuring better quality.
- Documentation that SDLC stresses on, is an important measure of communication & control.
- The phases are important milestones that help the project manager & the user for review & signoff.

4. Outline the advantages of SDLC Methodology from the viewpoint of IS Audit. Nov 2010,Nov 2012

Ans. (i) On the basis of detailed documentation created during each phase of SDLC, The IS Auditor can have **clear understanding of various phases of SDLC.**

(ii) On the basis of his examination,The IS Auditor can state in his report about the **compliance of procedures by IS mgt**.

(iii) On the basis of technical knowledge & ability of the area of SDLC,the **IS Auditor can be a Guide** during the phases of SDLC.

(iv) The IS Auditor can provide an evaluation of the methods & techniques used through the various development phases of the SDLC.

5. What are the risks associated with SDLC?

Ans. (i) The development team may find it cumbersome.

(ii) The user may find that the end product is not visible for a long time.

(iii) The rigidity of the approach may prolong the duration of many projects.

(iv) It may not be suitable for small & medium sized projects.

6. Bring out the reasons as to why the firms fail to achieve their system development objectives? RTP Nov 2003

Ans. 1. Lack of senior mgt support & involvement in info system development

2. Lack of user participation

3. Lack of standard project mgt & system development methodologies

4. New technologies 5. Shifting user needs 6. Overworked or under-trained development staff

7. Resistance to change 8. Inadequate testing & user training 9. Unstructured strategic decision-making

7. Explain the various Approaches to System Development in detail. {V.Imp}

Approach	Concepts

Waterfall (linear)

RTP May 2012

Basic Principles:

1. **Division of project into sequential phases:** The project is divided into sequential phases and some overlap & splash back is accepted b/w the phases.
2. **Emphasis:** The emphasis is given on planning,time schedules,target dates,budgets & implementation of the entire system at one time.
3. **Maintaining Tight Controls:** Tight are maintained over the life of the project **through -**
   - the use of extensive written documentation
   - Formal reviews & approval signoff by the user and
   - IT mgt (occurring at the end of most phases before beginning of next phase)

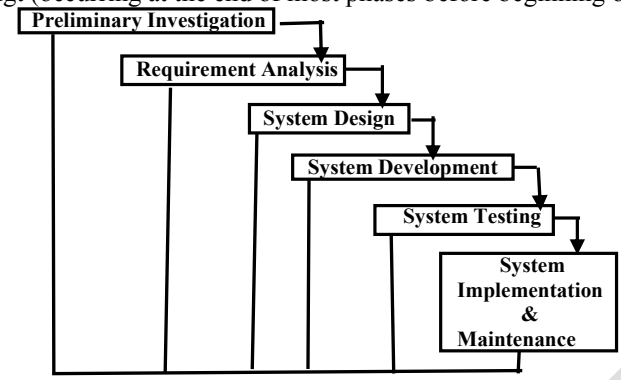


Fig. Steps in Traditional Approach

Strengths: (i) An orderly sequence of development steps ensure the quality,reliability,adequacy & maintainability of the developed software.
(ii) Ideal for supporting less experienced project teams & project managers or for project team whose composition fluctuates.
(iii) Progress of system development is measurable.
(iv) Conserve Resources.

Weaknesses: (i) Inflexible,slow,costly & cumbersome due to tight controls.
(ii) Project moves forward with little backward movement.
(iii) Problems are often not discovered until system testing.
(iv) System performance can't be tested until the system is fully coded.
(v) Difficult to respond to changes that occur later in the life cycle.

Prototyping (Iterative)

RTP May 2012; {May 2013}

Basic Principles: Prototyping can be viewed as a series of four steps which are :

Step 1 - Identifying info system requirements: Under Prototyping approach,the design team requires only the fundamental system requirements to build the initial prototype.The process of determining these requirements is less formal & less time-consuming under this approach as compared to that under traditional approach.

Step 2 - Developing the Initial Prototype: In this step,the designers create an initial base model & give little or no consideration to the internal controls but instead emphasize such system characteristics such as simplicity,flexibility & ease of use.

Step 3 - Testing & Revision: After finishing the initial prototype,the designers first demonstrate the model to the users & then give it to them to experiment & ask users to record their likes & dislikes about the system & recommend changes.

Step 4 - Obtaining user signoff of the approved Prototype: At the end of Step 3,users formally approve the final version of the prototype,which commits them to the current design & establishes a contractual obligation about what the system will & will not do or provide.

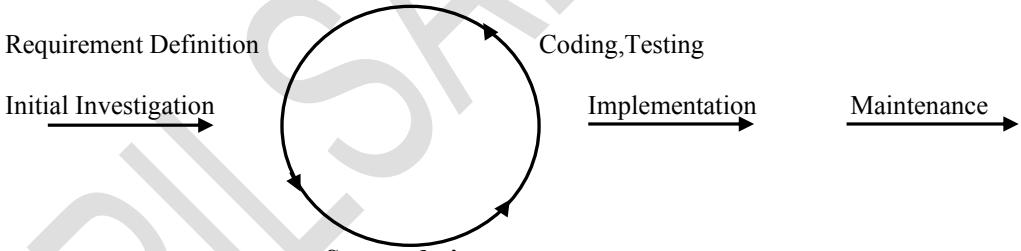


Fig. Prototyping Model

Strengths: (i) It improves the user participation in system development.
(ii) It is useful in determining user's exact requirements from the system.
(iii) It encourages innovation & flexible designs.
(iv) It provides quick implementation of an incomplete but functional application.
(v) Errors are detected & eliminated early in the developmental process.

Weaknesses [RTP May 2014]: (i) Prototyping can only be successful if the system users are willing to devote their significant time in experimenting with the prototype & provide the system developers with change suggestions,But it may possible that the users may either be not able or not willing to spend their time for such purpose.
(ii) Prototype may not have sufficient checks & balances incorporated.
(iii) Frequent changes in user requirements may cause delay or over cost the system.
(iv) Prototyping may cause behavioral problems with system users like - Dissatisfaction by users if the system developers are unable to meet all user needs/demands; Dissatisfaction & impatience by users when they have to go through too many interactions of the prototype.
(v) Sometimes,the system designers build prototype too quickly,without sufficient upfront user needs-analysis resulting in an inflexible design that limits future system potential.

Incremental (Combination of Linear & Iterative)

Basic Principles: Under this approach,the system is designed,implemented & tested incrementally, until it is finished.The product is decomposed into a no. of components,each of which are designed & built separately.Each component is delivered to the client when it is complete.Thus,this approach allows partial utilization of product & avoids a long development time.Under this approach,**system may be developed in any of the following ways**:

(i) A series of mini-waterfalls may be performed,where all the phases of system development are completed for a small part of the system,before proceeding to the next increment. **or**
(ii) Overall requirements may be defined before proceeding to the evolutionary,mini-waterfall development of individual increments of the system. **or**
(iii) The initial software concept,requirement analysis and design of architecture & system core may be defined using the waterfall approach,followed by iterative prototyping,which culminates in installation of the final prototype i.e the working system.

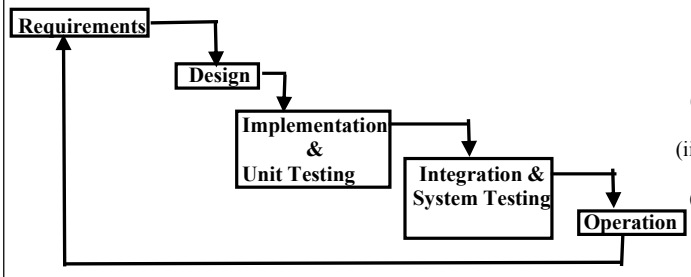


Fig. Incremental Model

Strengths:
(i) The effects of incremental changes,isolated issues etc are noticed earlier in the project which assists in making necessary adjustments before the organisation is adversely affected.
(ii) The knowledge gained in earlier increments are used in developing later increments.
(iii) It helps to mitigate the risks of integration & architecture earlier in the project.
(iv) Less costly to change scope & requirements. (v) More Flexible
(vi) The stakeholders may be provided the evidence of project status throughout the life cycle.

Weaknesses: (i) Each phase of iteration is rigid & do not overlap each other.
(ii) Well-defined interfaces are required due to early development of some of the modules.
(iii) Difficult problems may be pushed to the future to demonstrate early success to the management.
(iv) There may be lack of overall consideration of the business problem & technical requirements **for the overall system** because of utilizing a series of mini-waterfalls **for a small part of the system.**

Spiral Model (Combination of Linear & Iterative)

{Nov 2010}

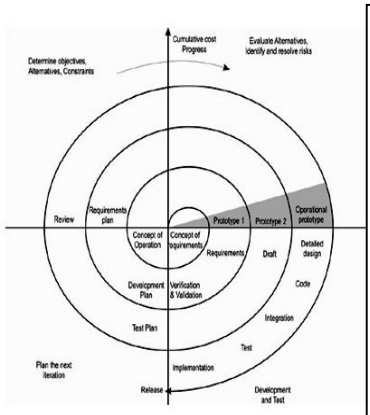


Fig. Spiral Model

Basic Principles: **RTP May 2013**
1. **Defining New System Requirements -** The new system requirements must be defined in as much detail as possible. It involves interviewing a no. of users representing all the external or internal users & other aspects of the existing system.
2. **Creating a Preliminary Design for new system -** Under this phase,all possible alternatives that can help in developing a cost effective project,are analysed & strategies are decided to use them.This phase also helps to identify & resolve all the possible risks in the project development.
3. **Constructing First Prototype -** A first prototype of new system is constructed from the preliminary design.This is usually a scaled-down system & represents an approximation of the characteristics of the final product.
4. **Constructing Second Prototype -** Procedure for constructing second prototype is as follows:
(i) Evaluating the first prototype in terms of its strengths.weaknesses & risks;
(ii) Defining the requirements of the second prototype;

Strengths: (i) It enhances the risk avoidance.
(ii) On the basis of project risk ,this approach can be useful in :
- Selecting the best methodology to follow for development of a given software iteration ;
- Incorporating the Waterfall,Prototyping & Incremental methodologies in the framework and providing guidance as to which combination of these models best fits a given software iteration.

Weaknesses: [RTP May 2014] (i) Since this approach is highly customized to every project,so it has limited re-usability.
(ii) A skilled & experienced project manager is required to determine how to apply it to a given project.
(iii) There are no established controls for moving from one cycle to another cycle.without controls,each cycle may generate more work for the next cycle.
(iv) Due to no firm deadlines,cycle continues with no clear termination condition,so there is an inherent risk of not meeting the budget or schedule.

Rapid Application Development (RAD) - Iterative

Basic Principles: (i) The project is divided into smaller segments which provides more ease-of-change during the development process.
(ii) It aims to provide a high quality software rapidly,primarily through the use of :
- ❖ Iterative Prototyping
- ❖ Active User-involvement
- ❖ Computerized Development Tools such as - GUI builders,CASE tools,DBMS,Fourth generation programming languages,Code generators & Object-oriented techniques etc.

(iii) This approach generally includes **Joint Application Development (JAD)**,where users are involved in system design **either** through consensus building in structured workshops **or** through electronically facilitated interaction.
(iv) The key emphasis is on fulfilling the business needs,while technological or engineering excellence is less important.
(v) The documentation required to facilitate the future development & maintenance are produced.
(vi) A functioning software is produced iteratively rather than producing a throwaway prototype.
Key Objective: Fast development & Delivery of a high quality system at a relatively low investment cost.
Strengths: (i) The operational version of an application is available much earlier than with Waterfall,Incremental or Spiral frameworks.
(ii) Low development cost due to quick production of working system.
(iii) Quick initial reviews are possible.

	(iv) It provides the ability of rapidly change the system design when demanded by the users. (v) It provides for saving in time,money & human effort. **Weaknesses:** (i) More speed & lower cost may lead to a lower overall system quality. (ii) Due to missing info,there is always a danger of misalignment of developed system with the business. (iii) Project may end-up with more requirements than needed (Gold-Plating). (iv) There is always a tendency for difficult problems to be pushed to the future to demonstrate early success to management. (v) Since some modules develop much earlier than others,therefore,well-defined interfaces are required. (vi) Modules developed are difficult to reuse for future systems.
Agile Methodology (Iterative & Incremental)	**Meaning:** It is a group of software development methodologies based on iterative & incremental development involving collaboration between teams.It promotes adaptive planning & encourages rapid & flexible response to change..It is a conceptual framework that promotes foreseen interactions throughout the development life cycle. **Basic Principles:** **RTP Nov 2012, RTP Nov 2013** (i) Simplicity (vi) Continuous attention to technical excellence & good design (ii) Self-organising teams (vii) Customer satisfaction by rapid delivery of useful software (iii) Regular adaptation to changing circumstances (iv) Welcome changing requirements,even late in development life cycle. (v) Face-to-Face Conversation & close co-operation between developers & users **Strengths:** **Nov 2013** ❖ This methodology has the concept of an adaptive team,that is why,it is able to respond to the changing requirements. ❖ Quick delivery of product without requiring to invest much time & effort even when the users requirements are changing. ❖ Face to Face communication & continuous inputs from customer representative leaves **no space for guesswork.** ❖ Clearly defined & to the point documentation saves time. ❖ The end result is the **High quality software in least possible time** that ensures customer satisfaction. **Weaknesses: [RTP May 2014]** ❖ In case of large software deliverables,it becomes difficult to assess the efforts required at the beginning of the software development life cycle. ❖ There is lack of emphasis on necessary designing & documentation because the team focuses on verbal communication with the customer rather than on documents or manuals. ❖ **Agile requires more re-work** when (i) There is lack of long term planning & lightweight approach to architecture and (ii) when the various components of the software are combined & forced to interact. ❖ The project can get taken off-track if the customer representative is not clear about the final outcome that they actually require. ❖ Only senior programmers are capable of taking right decisions during the development process,so,there is no or less scope for newly appointed programmers unless they are combined with experienced resources.

8. State & briefly explain the six stages of system development life cycle (SDLC) Nov 2008

Ans. SDLC: It is a set of six activities which ars closely related to each other.After a certain stage,these activities can be done parallel to each other.The six stages of SDLC are briefly explained below:

1. **Preliminary Investigation:** When the user comes across a problem in the existing system or a totally new requirement for computerization,a formal request has to be submitted for system development.It consists of three parts: **Request classification,Feasibility study and Request approval.**Feasibility study is conducted after the receipt of request & identification of needs are carried out.It includes the aspects related to Technical,Economic & Operational feasibility and is normally conducted by a third party depending upon the quantum & size of the requirements.The Approval is sought from Top mgt to initiate the system development.
2. **Requirement Analysis or System Analysis:** Once the request of the system development is approved,the detailed requirement study is conducted in the close interaction with the concerned employees & managers.
3. **System Design:** Under this activity,the system analyst designs the various procedures,report,inputs,files & database structures and prepares the comprehensive system design.These specifications are then passed on to the development team for program coding & testing.
4. **Acquisition & Development of Software:** Once the system design details are resolved & SRS is accepted by the user,the hardware & software details along with service requirements are determined & procured choosing the best-fit options.Subsequently,choices are made regarding which products to buy or lease from which vendors.
5. **System Testing:** Once all the programs comprising the system have been developed & tested,the system needs to be tested as a whole in a order to ensure that it does not fail in any condition.
6. **Implementation & Maintenance:** After accomplishment of above activities and ensuring that the requisite hardware & software are installed & the users are trained on the new system to carry out operations independently,the system is implemented and it is maintained & modified to adapt to the changing needs of the users.

9. What are the Steps involved in Preliminary Investigation?

Ans. 1. **Identification of problem:** (i) The first step in an application development is to **define the problem** clearly & precisely (ii) Next step is **assessing the prevalence of problem within organisation**.A problem that has considerable impact on the organisation is likely to receive immediate mgt action.
(iii) **Need for new system** may arise due to shifting business requirements,changing organisational environments & evolving IT.
(iv) If the need seems to be genuine,the **System analyst will submit all proposals to the Steering Committee** for evaluation to identify those projects that are most beneficial to the organisation.
2. **Identification of Objective:** After the identification of problem,it is easy to work out the objectives of the proposed solution. **For instance-**The problem of Railways was the inability to provide a convenient reservation system for a large no. of intending passengers.So its Objective should be "to provide a system wherein intending passengers could book a ticket from source to destination,faster than in a real-time."

3. **Delineation of Scope:** (Delineating means describing precisely) The scope of a solution defines its boundaries. It should be clear & comprehensive to the user mgt stating what will be addressed by the solution & what will not. Hence,outlining the scope in the beginning is essential.**The following questions should be answered while stating the scope: (Separate Question may be asked)**
(i) What functionalities will be delivered through the solution?
(ii) What data is required these functionalities?
(iii) What are the control requirements for this application?
(iv) What level of response time,execution time & throughput is required?
(v) What are the conditions,the input data has to conform?
(vi) Is there any special hardware/software that the application has to interfaced with?

While eliciting/obtaining info to delineate the scope,following aspects need to be kept in mind: RTP Nov 2012, RTP Nov 2013

(i) Different users will represent the problem & required solution in different ways.Therefore,the system developer should elicit the need from the initiator of the project who may be the member of the senior mgt.
(ii) An understanding of the profile of users at operating level helps in designing appropriate user interface features.
(iii) The development organisation has to clearly quantify the economic benefits to the user organisation.But other factors should also be given weight-age.**For Example-**In a security system,how foolproof (means unable to go wrong) it is may be a critical factor.
(iv) An understanding of the impact of the solution on the organisation is also necessary.
The two primary **Methods with the help of which the scope of the project can be analysed** are as follows: {**RTP May 2013**}
(i) **Reviewing internal documents:** The analysts conducting investigation try to learn about the organisation *involved in or affected by* the project.They can learn these details by examining organisation charts & studying written operating procedures.**Written documents tell the analyst how the system should operate.**
(ii) **Conducting Interviews:** Analysts conduct interviews to know more about the nature of the project request & the reasons for submitting it.

4. Feasibility Study (June 2009): After possible solution options are identified,the project feasibility is determined by the system analyst.It refers to a process of evaluating alternative systems through cost-benefit analysis so that the most feasible & desirable system can be selected for development.

What may be the possible dimensions under which the feasibility study of the proposed system may be evaluated? RTP May 2014

The dimensions under which the feasibility study of proposed system may be evaluated are as follows:

- **Technical:** Is the technology needed available?
- **Financial:** Is the solution viable financially?
- **Economic:** Return on investment?
- **Schedule/Time:** Can the system be delivered on time?
- **Resources:** Are human resources reluctant for the solution?
- **Operational:** How will the solution work?
- **Behavioral:** Is the solution going to bring any adverse effect on quality of work life?
- **Legal:** Is the solution valid in legal terms?

The following issues are typically addressed in the feasibility study: RTP Nov 2012, RTP May 2013

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

The feasibility study of a system is evaluated under following dimensions:

(i) **Technical:** It is concerned with hardware & software.The technical issues usually raised during the feasibility stage of investigation are as follows;

- Does the necessary technology exist to do what is suggested (and can it be acquired)?
- Does the proposed equipment have the technical capacity to hold the data required to use the new system?
- Will the proposed system provide adequate responses to inquiries regardless of no. or location of users?
- Can the system be expanded if developed?

(ii) **Economic Feasibility:** It includes an evaluation of all the costs & benefits expected if the proposed solution is implemented.The financial & economic questions raised by analysts during the preliminary investigation are as follows:

- The cost of conducting system investigation.
- The cost of hardware & software needed.
- The benefits in the form of reduced costs.
- The cost if nothing changes.

(iii) **Financial Feasibility:** The proposed solution may be costly which may be acceptable for an organisation with high turnover but may not be a viable solution for small organizations.
(iv) **Operational Feasibility:** **RTP Nov 2013**
It is concerned with ascertaining the views of workers,employees,customers & suppliers about the use of computer facility.Some of the questions which help in testing the operational feasibility of a project are as under:

- Is there sufficient support for the system from mgt/users?
- Is there any resistance for use of proposed system?
- Are current business methods acceptable to users?
- Will the proposed system produce poorer results in any aspects or areas?

(v) **Schedule Feasibility:** It involves the design team's estimation on how long will it take a new system to become operational & communicated this info to the steering committee.
(vi) **Legal feasibility:** It is concerned with whether there will be any conflict between a newly proposed system & the organisation's legal obligations.
(vii) **Resources Feasibility:** This focuses on human resources.Implemented sophisticated software solutions become difficult in non-metro locations because of reluctance of skilled personnel to move to such locations.
5. **Reporting results to Mgt:** After describing the problem & its scope,the system analyst proves one or more solution alternatives & estimates the cost & benefits of each alternative & reports these results to the mgt.From the analyst's report,mgt should determine what to do next.From the projects submitted for evaluation & review,the projects that meet the selection criteria are accepted & requests that fail to pass the feasibility test are re-worked & re-submitted as new proposals.

10. Explain the concept of cost Benefit Analysis during Preliminary Investigation. {Nov 2005}

Costs	Benefits that can result from the development of Computerized system {May 2012}
Development Costs: For a CBIS,development costs include costs of system development process,**such as** (i) Salaries of system analysts & computer programmers who design & program the system. (ii) Costs of converting & preparing data files and preparing system manual & other supportive documents (iii) Costs of preparing new or expanded computer facilities. (iv) Costs of testing & documenting the system,training employees & other start up costs. **Operating Costs:** For a CBIS,this costs include: (i) Hardware/Software rental or depreciation charges (ii) Salaries of Computer Operators & other data processing personnel who will operate the new system. (iii) Salaries of System Analysts & Computer Programmers who perform the system maintenance. **Intangible Costs:** Such costs can not be easily measured.**For example:** (i) The development of new system may disrupt the activities of an organisation & cause a loss of employee productivity or morale. (ii) Customer sales & goodwill may be lost by errors made during the installation of new system.	**Tangible Benefits** are those that can be accurately measured & are directly related to the introduction of new system,like- (i) **Decrease in** ➢ Data processing costs ➢ Operating costs ➢ Required Investments (ii) **Increase in** ➢ Sales or profits ➢ Operational ability & efficiency (iii) **Improved** ➢ Info availability ➢ Abilities in computation & analysis ➢ Customer Service ➢ Employee Morale ➢ Mgt decision-making ➢ Competitive position **Intangible Benefits** are harder to measure & define but they should be used in monetary terms to use them in financial reports. **Eg.** Improved Business Image

11. What are the activities to be performed during System Requirement Analysis Phase? May 11;May 13;RTP May 2012 &2014

Ans. (i) Identifying & consulting the stake owners to determine their expectations & resolving their conflicts.
(ii) Analyzing requirements to detect & correct conflicts and determining the priorities.
(iii) Verifying that the requirements are complete,consistent,verifiable,modifiable,testable & traceable.
(iv) Gathering the data or finding facts using tools like- Interviewing,Questionnaires,Observation etc.
(v) Documenting activities such as Interview,Questionnaire,Reports etc & Developing a System (Data) Dictionary.
(vi) Developing Models to document Data Flow Diagram etc.

12. Briefly discuss various Fact Finding Techniques used by the System analyst for Determining the Users'requirements / needs of the organisation. May2010, RTP May 2014

Ans. Every system is built to meet some set of needs.To assess these needs,the Analysts often interact with the people (who will be benefited from the system) in order to determine their actual requirements.Various Fact Finding Techniques are as under:
1. **Documents:** These are the good source of info about user needs & the current system.These includes:
- Manuals,Input forms,Output forms,Diagrams - showing how the current system works.
- Organisation Charts - showing the hierarchy of users & manager's responsibilities.
- Job description of the people - who work with the current system
- Program codes - for the applications associated with the current system.

2. **Questionnaires:** These are the set of pre-decided questions about the working of info system.These are given to the users & managers to fill,in order to obtain their responses from the info system.
3. **Interviews:** Users & managers may also be interviewed to obtain info in detail.The data gathered through the interviews provide the system developer with a complete picture of the problems & opportunities.
4. **Observation:** In Prototyping approaches,observation plays an important role in the requirement analysis.Only by observing users' reaction to the prototypes,the system developer can develop a better system.

13. Discuss in brief,the various functional areas to be studied by a system analyst for a detailed investigation of Present System. {May 2011,Nov 2011}

Ans. Detailed investigation of present system involves collecting,organising & evaluating facts about the system & the environment in which operates.Appropriate Info should be gathered so as as to enable a qualified person to understand the present system without visiting any of the operating departments.For this purpose,following areas should be studied in depth:
1. **Review Historical Aspects:** A brief history of the organisation is the starting point for an analysis of the present system.The System analyst should review Annual Reports,Organisation Charts etc to identify the growth of mgt levels,development of

various functional areas & departments.He should investigate what system changes have occurred in past that have been successful or unsuccessful with computer equipment & techniques.

2. **Analyze Inputs:** Analyses of present inputs are the basis for manipulation of data.The system analyst should be aware of the various sources from where the data are initially captured since the outputs for one area may serve as an input for another area.

3. **Review Data-files maintained:** The system analyst should investigate the data-files maintained by each deptt,noting their no. & size,where they are located & used.Such info may be contained in system & procedure manuals.He should also review all on-line & off-line files as it reveals info about data that are not contained in any outputs.

4. **Review Methods,Procedures & Data Communications:** A Method is defined as "a way of doing something" and Procedure is defined as "a series of logical steps by which a job is accomplished".

A **procedure review** is an intensive survey of :	**Data Communication review** involves reviewing :
➢ The methods by which each job is accomplished ➢ The equipment utilized and ➢ The actual location of the operations. Its basic Objective is to eliminate un-necessary tasks or to perceive important opportunities in the present IS.	(i) Data interface (iii) Modems (v) Leased lines and (ii) Data links (iv) Dial-up (vi) Multiplexers Its basic Objective is to understand how the data - communication network is used in the present system so as to identify the need to improve the network when the new system is installed.

5. **Analyze Outputs:** Its Objective is to determine how well the outputs or reports meet the organisation's needs.The system analyst must understand what info is needed & why and when & where it is needed.Reports carried over from earlier years that have no more relevance,should be eliminated in the new system.

6. **Review Internal Controls:** Such review helps the system analyst to visualize the essential parts & framework of a system.An examination of the internal controls of the present system may indicates the weaknesses that should be removed in the new system.

7. **Model the existing physical system & logical system:** The system analyst should prepare the system flow charts,data flow diagrams etc as these diagrams/models help to present the complete description of the existing system in terms of data flows,processes & outputs.

8. **Undertake overall analysis of present system:** Based upon the aforesaid investigation of the present info system,the final phase of the detailed investigation includes the analysis of :

- The present work volume
- The current personnel requirements and
- The present costs & benefits

Each of these must be investigated thoroughly.

14. How is the System Analysis of a Proposed System is carried out?

Ans. After each functional area of the present info system has been carefully analysed,the proposed system specifications must be clearly defined.Consideration should be given to the strengths & weaknesses of the present system.

The required system specifications (i.e set of requirements to be satisfied by proposed system) which should be in conformity with the project's objectives **are as follows:**

- **Outputs** should be produced with great emphasis on timely managerial reports.
- **Database** should be maintained with great emphasis on on-line processing capabilities.
- **Input data** should be prepared directly from the original source documents for processing by the computer system.
- **Methods & Procedures** should show the relationship of inputs & outputs to the database wherever required.
- **Work volumes & timings** should be carefully addressed for present & future periods including past periods.

Procedure/Steps for compiling these specifications are as under:

- Determine Outputs
- Determine Inputs,database,methods,procedures & data communications to be employed.

The **Output-to-input** process is recommended since outputs are related directly to the objectives of the organisation.

15. Discuss some of the System Development Tools widely used by System analysts.

Ans. **Use of System Development Tools:** These tools help the system analyst to :

- improve current info system & to develop new info system.
- Analyze present business operations,mgt. decision-making & info processing activities of the organisation.
- Propose & design new or improved info systems to solve business problems.

Types/Categories of System Development Tools:

1. **System Components & Flows:** These tools help the system analysts to document the data flow among the major resources & activities of an info system.Tools used under this category are:

(i) **System Flowcharts:** It is a graphic technique used to represent the inputs,outputs & processes of a business in a pictorial form.Under this technique,a chart is prepared to represent an algorithm or process showing the steps as boxes of various kinds & their order by connecting these with arrows.

(ii) **Data Flow Diagrams:** A DFD uses a few simple symbols to illustrate the flow of data among external entities.A DFD is composed of four basic elements,that are:

Symbol	Name	Explanation
	Data sources & destination	Sending data to/from the system is represented by square boxes called data sources or data sinks.
	Data flows	The flow of data into or out of a process is represented by curved or straight lines with arrows.
	Transformation process	The processes that transform data from inputs to outputs are represented by circles,often called Bubbles.
	Data stores	The storage of data is represented by two horizontal lines.

(iii) **System Components Matrix:** It provides a matrix framework to document the resources used,the activities performed & the info produced by the info system.It highlights how the basic activities of input,processing,storage,output & controls are accomplished in an info system and how the use of hardware,software & people resources can convert data resources into info products.

2. **User Interface:** Designing the interface between end-user & the computer system is a major consideration of a system analyst while designing the new system.Tools under this are:

(i) **Layout forms & screens:** This tool helps to design user interface and provides a layout base to design input forms & output reports.This tool is also known as **Report Generator** or **Form Generator.**

(ii) **Dialogue flow diagram:** It helps to analyze the flow of dialogue b/w user & the computer.

3. **Data Attributes & Relationships:** These tools help to define,catalogue & design the data resources in the info system.Tools under this are:

(i) **Data Dictionary: {May 2012}** It is a computer file that contains descriptive info about the data items in the files of a business info system.This info may include the following:

- **Identity of source documents -** that are used to create the data items.
- **Names of computer files -** that store the data items.
- **Names of computer programs -** that modify the data items.
- **Identity of computer programs or individuals -** who are permitted/not permitted to access the data items for the purpose of file maintenance,upkeep or inquiry.
- **Additions/Deletions to the record structure -** When the new data fields are added to the structure of a business file,then the info about each new data item is used to create a new computer record in the data dictionary.When the data fields are deleted from the structure of file records then their corresponding records are dropped from the data dictionary.

Use of Data Dictionary for Accountants & Auditors:

- When an Accountant participates in the design of a new system,he can use the data dictionary to plan the flow of transaction data through the system.
- An Auditor can use the data dictionary to establish an audit trail because it can identify the input sources of data items,the computer programs that modify particular data items & the managerial reports on which the outputs are based.

(ii) **Entity-Relationship Diagram:** It documents the no. & type of relationship among the entities in a system.

(iii) **File Layout Forms:** It documents the type,size & names of the data element in a system.

(iv) **Grid Charts:** It helps in identifying the use of each type of data element in Input/Output or Storage media of a system.

4. **Detailed System Process:**These tools are used to help the programmer to develop detailed procedures & processes required in the design of a computer program.Tools under this are:

(i) **Decision Trees:** It is commonly used in operations research (O.R) as a tool to identify most appropriate strategy which will help to achieve goals under different conditions.It is a tree-like graph which provides sequence of decisions with possible consequences.

(ii) **Decision Tables:** It is a table which may accompany a flowchart defining the contingencies within a program & appropriate course of action for each contingency.It defines a logical procedure by means of a set of conditions & the related actions.

Parts of a Decision Table:

- **Condition Stub:** It lists out the conditions or comparisons that could exist in a program.
- **Action Stub:** It lists statements that describe all the actions that can be taken.
- **Condition Entries:** It indicates which conditions are being met or answer the questions in the condition stub and also describes which factors are actually the components of a decision.
- **Action Entries:** It specifies the actions to be taken & defines the actual results of the decision.

(iii) **Structure Charts:** It documents the purpose,structure & hierarchical relationships of the modules in a program.

16. Write short notes 'Pseudo Code' and 'CASE Tools'.

Structured English or Pseudo Code	CASE Tools
(i) It refers to the use of english language with the syntax of structured programming. (ii) It aims at getting the benefits of both the programming logic & natural language. (iii) Programming logic helps to attain precision and (iv) Natural language helps in getting the convenience of spoken languages.	(i) CASE stands for Computer-Aided-Software-Engineering. (ii) It refers to the automation of anything that humans do to develop systems & support virtually all phases of traditional system development process. (iii) Some of the **features** that various CASE products possess are : *Data Dictionary,Computer aided diagramming tools,word processing,screen & report generator,prototyping,project management,code generation;and Reverse Engineering.* (iv) On-screen drawing modules found in CASE software packages are commonly used by the users to generate Data Flow Diagram & System Flow Charts.

17. At the end of Analysis Phase,the System Analyst prepares a document called "System Requirement Specifications (SRS)".Write the contents of SRS.

Ans. A SRS contains the following:

- **Introduction:** It describes about the system to be developed with its goals & objectives.
- **Info Description:** It describes the info content required with flowcharts & structure and describes about hardware,software,human interfaces for external system elements & internal software functions.
- **Functional Description:** It describes about all the functions to be performed by the system in a diagrammatic representation with processing narrative for each function.

- **Behavioral Description:** It describes about the response to external events & internal controls.
- **Validation Criteria:** It describes about the classes of tests to be performed to validate functions;performance & constraints.
- **Appendix:** It provides the detailed description of algorithm charts,graphs,data flow/object diagrams,tabular data & other such material.
- **SRS Review:** It reflects the development team's understanding of the existing processes and It contains the following:

* The development team makes a presentation & then hands over the SRS document to be reviewed by the user/ customer.

* The user should sign the document only after ensuring that the document represents the existing processing accurately as user's sign on the document is a technical requirement of the contract b/w the users & the development team/organisation.

18. Explain the various steps involved in the System Design phase.

Ans. 1. **Architectural Design:**

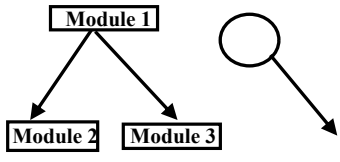


Fig. Functional Decomposition Tool

(i) This design is made with the help of **"Functional Decomposition Tool"** which has three elements -
* Module - It is represented by a box.
* Connection - The connection b/w modules is represented by arrows.
* Couple - It is a data element that moves from one module to another module & is shown by an arrow with circular tail.
(ii) Architectural design deals with the organisation of applications in terms of hierarchy of modules & sub-modules.At this stage,system designers identify -

- Major modules
- Function & scope of each module
- Interface features of each module
- Direct & indirect linked module etc.

2. **Design of Data/Info Flow:** This is the major step in the conceptual design of new system.In designing the data/info flow for the proposed system,the inputs required are - (i) Existing data/info flows (ii) Problems with the present system and (iii) The Objectives of new system.

3. **Design of Database:** It involves determining its scope ranging from local to global structure.The design of database involves four major activities which are discussed below: **May 2012**

Design Activity	Explanation
Conceptual Modeling	This activity describes (i) The application domain via entities/objects (ii) Attributes of these entities/objects and (iii) Static & Dynamic constraints on these entities/objects,their attributes & their relationships.
Data Modeling	Under this activity,conceptual models are translated into data models so that they can be accessed & manipulated by both high level & low level programming languages.
Storage Structure Design	In this activity,decisions are taken on how to partition the data structure so that it can be stored on some device.
Physical Layout Design	In this activity,decisions are taken on how to distribute the storage structure across specific storage media & locations.

4. **Design of User-interface:** It involves determining the ways in which the users will interact with the system.The points that need to be considered while designing the user-interface are :

(i) Source Documents - to capture the raw data
(ii) Hard copy output reports
(iii) Screen Layouts - for dedicated source-document input
(iv) Inquiry Screens - For database interrogation
(v) Graphic & color displays etc.

5. **Physical Design:** (i) For the physical design,the logical design is transformed into units which in turn can be further decomposed into implementation units such as programs & modules.

(ii) During physical design,the primary concern of the auditor is effectiveness & efficiency issues.

(iii) Some of the issues addressed here are -

a) Type of hardware - for client application & server application
b) Operating system to be used
c) Type of networking
d) Processing - batch,online,real time
e) Frequency of input,output

6. **Design of the Hardware/system Software platform:** (i) If the hardware/system software required by new system is not currently available in an organisation,then,such hardware/system software platform will have to be designed.

For example: A DSS might require high-quality graphics which may not be supported by the existing hardware & software.

(ii) If different hardware & software are not able to communicate with each other then subsequent changes will have to be made to make the hardware & software compatible to each other.

19. List the important factors to be considered by the System Analysts while designing user input/output forms.

Aspect	Definition	Input Design	Output Design
Content	It refers to actual pieces of data to be gathered to produce the required user output.	The Analyst should gather required data to generate desired user output. He may design new documents for collecting such info.	**Example** - Weekly report to a sales manager might consists of salesmen's name,sales calls made & product sold etc.
Timeliness	It refers to when users need output on regular/periodic basis **like** weekly,monthly,quarterly or annually.	Computer needs input data in time to produce output data..so,a plan must be established regarding when different types of data will enter into the system.	**Example** - (i) A sales manager may require a weekly sales report. (ii) Airline agents require both real-time info & rapid response times in order to provide better client service.
Format	(i) Input format refers to physical arrangement of data. (ii) Output format refers to the way in which the contents are	Output contents & media requirements are decided first,then input formats are designed on the basis of factors like -	Output formats like info reports should assists in decision-making,identifying & solving problems and initiative corrective action.

	displayed on output media.	a) Type & length of each data field b) Other special characteristics like no.,decimal places etc.	
Media	It refers to physical device used for I/O & Storage.	Various user input alternatives may include display workstations, keyboards,optical character recognition, voice input etc.	Output media may include Paper,Video display,Microfilm,Magnetic Tape/Disk and Voice Output.
Form	(i) Input Form is the way,the info is inputted and (ii) Output Form is the way,the info is presented to the users.	Input forms serve as source documents for the data entry personnel.**Example** - Pre-printed papers - that require the people to fill in responses in a standardized way.	Output forms should be decided based on user requirements. **Example** - Managers may require detailed info on some issues & summary info in other areas.

20. Mgt. should establish acquisition standards that address the same security & reliability as development standards.What should be the focusing areas of acquisition standards? RTP May 2013

Ans. After a system is designed either partially or fully,the next phase of the system development starts which relates to the acquisition of hardware,software & services.Mgt. should establish acquisition standards that address the same security & reliability as development standards.**Acquisition standards should focus on -**

- Ensuring that the security,reliability & functionality has already built into the product.
- Ensuring that the managers are entered into the contracts with appropriate vendors,have reviewed licensing and have acquired the products that are compatible with the existing systems.
- **Invitations-to-tender** (since these involve soliciting bids from vendors when acquiring h/w or integrated systems of h/w & s/w)
- **Request-for-proposals** (since these involve soliciting bids when acquiring off-the-shelf or third-party developed software)
- Ensuring that the functional,security & operational requirements are accurately identified & clearly detailed in the request-for-proposals.

21. Write short notes on Hardware Acquisition in the context of System Acquisition.

Ans. Hardware Acquisition: Procuring hardware is not an easy task due to rapid changes in technologies of hardware & software applications.It also requires a continuous support from vendors in terms of service & compatibilities with changing h/w technologies & software applications.**The following points should be considered before finalizing the computer hardware:**

1. The selection of h/w should be based on system design & technology selected that should satisfies the data processing requirements.
2. Hardware should be selected of latest technology.
3. Hardware should be procured to support the required inputs & output devices and can handle required type of data volume.
4. Hardware purchased should be easily expandable & upgradable in future for increased processing requirements.
5. There should be required support from hardware vendor both for operational as well as for technical requirements.

22. Write short notes on Software Acquisition in the context of System Acquisition.

Ans. After the input & output designs are finalized,the system analyst must understand the nature of application software requirements.At this stage,the system developers should determine whether the application software should be developed in-house or it should be acquired from the vendor.Buy decision for software should depends upon the following factors:

1. Required software is available in the market.
2. Time required to develop new software is not available with the mgt.
3. Cost of developing software is very high.
4. Skills required to develop software is either not available or available but very expensive.

23. Write short notes on Contracts,Software licenses & Copyright violations, in the context of Software Acquisition.

Ans. (i) Contracts b/w an organisation & software vendor should clearly describe the rights & responsibilities of the parties to the contract.The contracts should be in writing with sufficient detail to provide assurances for performance, s/w & data security etc.
(ii) Software license grants permission to do things with computer software that are otherwise prohibited by copyright law,patent law,trademark law and any other intellectual property right.
(iii) Copyright laws protect proprietary as well as open-source software.The use of unlicensed software or violations of a licensing agreement expose organizations to possible litigations.

24. List the factors to be considered for evaluation & selection of vendor's proposals. May 2006

Ans. Following factors should be considered for evaluation & selection of vendor's proposals:
(i) The Compatibility of each proposed system with the existing system;
(ii) The Performance capability of each proposed system in relation to its cost;
(iii) The Costs & Benefits of each proposed system;
(iv) The Maintainability of each proposed system ; and
(v) The Vendor's support.

25. Describe in brief, the methods of validating vendor's proposals. RTP May 2014

Ans. (i) **Checklists:**

In this method,a list is prepared for required specifications from system in terms of hardware, software & support services etc and the proposals are selected on the basis of this list.

An example of Support Service Checklist is given below:

Parameters	Vendor 1 (Dell)	Vendor 2 (IBM)	Vendor 3 (HP)
Performance	Excellent	Very Good	Good
Training Support	Provided	Provided	Provided
Back-up	Provided	Provided	Provided
Hardware	Excellent	Moderate	Good
Software	Excellent	Excellent	Good

(ii) **Point-Scoring Analysis:**

In this method,every evaluation criteria is given maximum possible points and then the points are allocated to each vendor for these criteria as per the submitted details in their proposals.The vendor who satisfies the given criteria is selected for acquiring system.

An Example of Point Scoring Analysis is given below:

Software Evaluation Criteria	Possible Points	Vendor A	Vendor B	Vendor C
Does the software meets all the mandatory specifications?	10	7	9	6
Does the software contain adequate controls?	10	9	9	8
Does the software have an adequate warranty?	8	6	7	6

(iii) **Public Evaluation Reports:** Several consultancy agencies compare & contrast the hardware & software performance for various manufacturers & publish their reports in this regard.This method is useful where the buying staff has inadequate knowledge of facts.

(iv) **Bench marking problem for vendor's proposals:** This is a practical approach for testing whether the computer offered by the vendor meets the requirements of the job on the hand of buyer.In this approach,a job mix of possible transactions to be executed on the required system is prepared & then the same is executed on the vendor's proposed system.Proposal will be accepted if the proposed system meets the requirements.

(v) **Test Problems;** In this approach,the test problems on certain issues (like the Time required to translate the source code into the object code,Response time for two or more jobs in multi-programming environment,Time required to execute an instruction etc) are developed and their relative weight age are assigned.Based on these test problems,the results achieved by the machine are compared & the price performance judgment can be made.

26. What are the features of a Good Coded Program? RTP Nov 2012, Nov 2012, RTP Nov 2013

Ans. A good coded program should have the following characteristics:

1. **Accuracy:** It refers not only to what a 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 & auditors.
2. **Efficiency:** It refers to the performance which should not be unduly affected with the increase in input values.
3. **Reliability:** It refers to the consistency which a program provides over a period of time.However,poor setting of parameters & hard coding could result in failure of a program after some time.
4. **Usability:** It refers to a user-friendly interface & easy-to-understand document for any program.
5. **Readability:** It refers to the ease of maintenance of a program even in the absence of a program developer.
6. **Robustness:** It refers to the process of taking into account all possible inputs & outputs of a program in case of least likely situations.

27. Explain in brief the various Steps/Stages/Activities involved in System Development Phase of SDLC.

Ans. 1. **Program Coding Standards:** These standards are set of rules that serve as a method of communication b/w teams,amongst team members & users.Different programmers may write a program using different sets of instructions but each giving the same results.These standards provide the following benefits :

- They minimize the system development setbacks (i.e delays or obstacles) due to programmer turnover.
- They provide simplicity,ensure efficient utilization of storage & take least processing time.

2. **Programming Language:** These are the set of instructions or program codes that are used by the system developers in writing software,statements or instructions which are then converted to binary by using compiler so that the computer can understand & execute the required instructions.The choice of programming language depends upon the application area;algorithm complexity;environment in which the software has to be executed; and the capability of in-house staff for maintenance etc.The most commonly used programming languages are as follows :

- High-level general purpose programming language such as COBOL and C language.
- Object-oriented languages such as C++,JAVA etc.
- Scripting language like JAVA Script,VB Script.
- Decision Support or Expert System languages like PROLOG.

3. **Program Debugging:** It is the most primitive (i.e earliest) form of testing activity which refers to correcting programming language syntax & diagnostic errors so that the program compiles cleanly.Steps involved in program debugging are as follows:

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

Eg. On writing the I.put,the compiler will correct it & re-submit it as Input.

4. **Program Testing:** In this step,the programmer plans the testing to be performed on each program so as to assess the success of installation of a system.The program test plan should be discussed with the project manager & the system users.A log should be kept for test results & conditions that are successfully tested.
5. **Program Documentation:** The writing of narrative procedures & instructions is done throughout the program life cycle.Managers & system users should carefully review the documentation in order to ensure that the software & the system behave in the same manner as the documentation indicates.If thy do not,the documentation should be revised.
6. **Program Maintenance:** The continual changing requirements of data processing applications require modification of various programs.Such modifications are generally done by maintenance programmers.

28. Explain in detail the different levels of testing during System Testing phase of SDLC.

Ans. Different levels of Testing are as follows:

1. Unit Testing: (i) 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.(ii) A unit test provides a strict written contract

that,the piece of code must satisfy. (iii) Unit tests are typically written & run by the system developers to ensure that the code meets its design & behaves as intended.(iv) In Computer programming,unit testing is a software verification & validation method,in which a programmer tests whether the individual units of source code are fit for use.(v) The goal of unit testing is to isolate each part of the program & show that the individual parts are correct.

Various Categories of tests that a programmer should typically perform on a program unit {RTP May 2013}

OR

Method to test the correctness of particular module of source code {Nov 2010}

OR

The Areas/Aspects of tests that can be performed on a Program Unit {May 2010}

(i) **Functional Tests:** These tests check whether programs do what they are supposed to do or not.The test plan specifies the operating conditions,input values & expected results, and the programmer checks by inputting the values to see whether the actual results & expected results match.

(ii) **Performance Tests:** Such tests should be designed to verify the response time,execution time,primary & secondary memory utilization and the traffic rates on data channels & communication links.

(iii) **Stress Tests:** Such tests are used to determine the stability of a given system or entity.It involves testing beyond normal operational capacity in order to overload a program for the purpose of determining the limitations of the program.

(iv) **Structural Tests:** These tests are concerned with examining the internal processing logic of a software system.

(v) **Parallel Tests:** In these tests,the same test data is used in the new system & old system in order to compare the output results.

Types of Unit Testing

(i) **Static Analysis Testing:** It does not involve any code execution.Some important static analysis tests are as follows:

a) **Desk Check:** This is done by the programmer himself.He checks for logical syntax errors & deviation from coding standards.

b) **Structured Walk-Through:** Under this,the application developer leads other programmers through the text of program & explanation.

c) **Code Inspection:** Under this,the program is reviewed with formal checklists by a formal committee.

(ii) **Dynamic Analysis Testing : RTP Nov 2013**

It involves actual testing of program with test data.Some important tests performed under this are as follows:

a) **Black Box Testing: (Nov 2009)** It takes an external perspective of test object to derive the test cases.These tests can be functional or non-functional.The test designer selects valid & invalid inputs to determine the correct output.There is no knowledge of test object's internal structure.

This method is applicable to Unit testing,System testing, and Acceptance testing.The higher the level of testing,the bigger & more complex will be the box.If a module performs a function which is not supposed to,the black box test does not identify it.

b) **White Box Testing:** It uses an internal perspective of the system to design test cases based on internal structure.It requires programming skills to identify all paths through the software.Since,the tests are based on actual implementation,if the implementation changes,the tests will also probably change.

This method is applicable at Unit,Integration, and System levels of testing process.While it normally tests paths within a unit,it can also test paths b/w units during integration and b/w sub-systems during a system level test.

c) **Gray Box Testing:** This technique uses a combination of black box testing & white box testing.Under this technique,the test designer uses the white box approach to apply a limited no.of test cases to the internal workings of the software under test and in the remaining part,he uses the black box approach in applying inputs to the software under test & observing the outputs.

2. **Integration Testing:** This testing is done after unit testing but before system testing.Under this testing,individual software modules are combined & tested as a group with an objective to evaluate the connection of two or more components that pass info from one area to another.

Types of Integration Testing RTP May 2012

(i) **Bottom-up Integration:** It is the traditional strategy used to integrate the components of a software system into a functioning whole.It consists of unit testing,followed by sub-system testing, and then testing of the entire system.

Advantage: Easy to implement.

Disadvantage: Major decision is deferred to a later period.

(ii) **Top-down Integration:** It starts with testing of main module & after completing its testing,stubs are substituted with real modules one by one and then these modules are tested with stubs.

Advantage: It emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes.

Disadvantage: Difficulties may arise because the high level modules are tested with outputs from stubs but not with the real outputs from subordinate modules.

(iii) **Regression Testing (Nov 2010) :** This testing is done when new modules are added to the existing modules,since each time a module is added as part of integration testing,the software changes.These changes may cause problems with functions that were previously worked perfectly.Regression tests ensure that changes or corrections have not introduced any new errors.The data used for regression tests should be the same as it was used in the original test.

3. System Testing: It is a process in which software & other system elements are tested as a whole.System testing begins either when the software as a whole is operational or when the well defined subsets of the software's functionality have been implemented.

Purpose of System Testing - It ensures that the new or modified system functions properly.

Types of System Testing RTP May 2012

(i) **Recovery Testing:** This testing is performed to determine the ability of application to recover from the crashes,hardware failures & other similar problems.

(ii) **Security Testing:** This testing is performed to determine the ability of info system to protect the data & maintain functionality as intended.Security testing must cover the following six concepts of security :
(a) Confidentiality, (b) Integrity, (c) Availability, (d) Authentication, (e) Authorization, and (vi) Non-Repudiation.
(iii) **Stress or Volume Testing:** This testing is performed to determine the stability of a given system.It involves testing beyond the normal operational capacity,often to a breaking point.
(iv) **Performance Testing:** This testing is performed to determine the speed or effectiveness of a computer,network,software program or device.

4. Final Acceptance Testing:

Explain 'Final Acceptance Testing' in brief. RTP May 2014

This testing is conducted when the system is just ready for implementation.This testing ensures that the quality standards adopted by the business & the system satisfies the users.

Types of Final Acceptance Testing

(i) **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 methodology,
(ii) **User Acceptance Testing:** It ensures that the functional aspects expected by the users have been well addressed in the new system.There are two types of user acceptance testing:

a) Alpha Testing: This is the first stage,often performed by the users within the organization.
b) Beta Testing: This is the second & last stage,generally performed by the external users after which the product is normally sent outside the development environment for real world exposure.

29. Describe the various Activities/Steps to be taken for the successful installation of Equipment during the System Implementation Phase of SDLC.

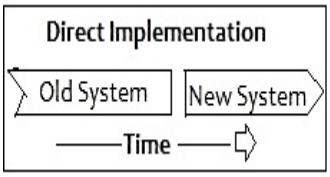
Ans. 1. **Equipment Installation:** The Hardware selected prior to the implementation phase to support the new system should be ordered in time so that the installation & testing of equipment could be made during implementation phase.Following steps are involved in equipment installation:
(i) **Site Preparation** - First of all, a site layout is prepared for users sitting arrangement,wiring arrangement, and for equipment setting etc. after thoroughly considering all the parameters like Temperature,Humidity & Dust control etc.
(ii) **Installation of new hardware/software** - The equipment must be physically installed by the manufacturer,connected to the power source and wired to the communication lines.If the new system interfaces with other systems or is distributed across multiple software platforms,then,some final commissioning tests of the production environment should be performed to check end-to-end connectivity.
(iii) **Equipment Check out** - To ensure proper working of equipment,it must be turned on and some extensive tests must be run on it.

2. Training Personnel: A system can succeed or fail depending on the way it is operated & used.That is why,when a new system is acquired,both users & computer professionals generally require some type of training.Therefore, the quality of training received by personnel helps or hinders the successful implementation of info system.

3. System implementation Conversion Strategies: Conversion or changeover is a process of changing from the old (manual) system to the new (Computerized) system.

Types of Implementation Strategies

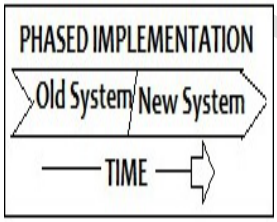
(i) **Direct implementation/Abrupt changeover** -



This is achieved through an abrupt takeover - an all or nothing approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go. Direct implementation usually takes place on a set date, often after a break in production or on a holiday so that the time can be used to get the hardware & software for the new system installed without causing too much disruption.

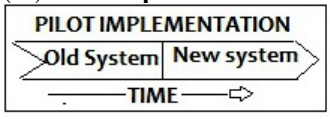
Difference between Phased Implementation & Pilot Implementation. RTP Nov 2012

(ii) **Phased Implementation** -



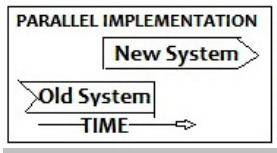
This approach is used when the same system is to be installed at many places. If the conversion of a system at one place is done successfully, then the same system can be installed at other places also.
Advantage: Problems detected in the initial installation can be avoided or removed in the subsequent installations.
Disadvantage: Successful conversion on one site may not work at other sites due to different requirements.

(iii) **Pilot Implementation** -



With this strategy, the new system replaces the old system in one oeration but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced & replicated throughout the whole system in good time with the least disruption. **For e.g.** It might be tried out in one branch of the company & if successful, then the pilot is extended until it eventually replaces the old system entirely.

(iv) **Parallel Running Implementation** - **[RTP May 2014]**



This is considered the most secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new system come online. With this strategy, the old system & the new system are both used alongside each other, both being able to operate independently. If all goes well, the old system is stopped & new system carries on as the only system.

30. Explain the major Conversion Activities involved in Conversion Procedure. {Nov 2010}

1. **Procedure Conversion** - Operating procedures should be clearly documented to assist the personnel in their functional areas. Info on input,data files,methods,procedures,output, and internal controls must be presented in clear, concise & understandable terms. Written procedures must be supplemented by oral communication during the training session on the system change.
2. **File Conversion [RTP May 2014]**- In this activity,the old data files are converted as per the new system requirements.It is done before the implementation of new system to make the old files compatible for new system.Old files should also be kept for some time because if any bug is detected later in the conversion routine,the same can be rectified.
3. **System Conversion** - After on-line & off-line files have been converted and the reliability of new system has been confirmed,the routine processing can be shifted to the new system.Old system should also be operated on for some time to compare the results of both the systems.
4. **Scheduling Personnel & Equipment -** For the maximum utilization of new system, the personnel & equipment must be scheduled by the system manager in conjunction with IT & departmental managers. Jobs should be allocated as per the equipment scheduling.

31. Write short notes on Post Implementation Review and Evaluation. {RTP Nov 2004}

Ans. PIR Meaning: PIR should be done after the solution has been deployed. It examines the effectiveness of all elements of the working business solution to see whether further improvements can be made to optimize the benefit delivered.

Purposes of PIR: PIR should be done - (i) To ascertain the degree of success from the project (ii) To deliver planned levels of benefit and (iii) To address the specific requirements as originally defined.

Aspects of Evaluation:

There are two basic dimensions of info system that should be evaluated,these are :
(i) Whether the newly developed system is operating properly? And
(ii) Whether the user is satisfied with the info system with regard to the reports supplied by it?

Types of Evaluation:

1. **Development Evaluation** - This evaluation is done to check whether the system has been developed on schedule & within budget. It requires schedules & budgets to be established in advance. If the system is not developed on schedule & within budget,then the possible reasons for delay & over cost etc are noticed & identified as evaluation remarks.
2. **Operation Evaluation** - This evaluation pertains to check whether the hardware,software & personnel are capable to perform their duties. It requires evaluation criteria to be established in advance.

For Example: If the system analyst has laid down a criteria that a system which is capable to support 100 terminals should give response time of less than 2 seconds, then the evaluation of this aspect of system operation can be done easily when the system becomes operational.

3. Information Evaluation - This evaluation pertains to evaluate the info provided by the info system. Since the objective of an info system is to provide info to support the organizational decision system, therefore, the extent to which the info system is supportive to decision making is the area of concern in evaluating the system. This aspect of system evaluation is however a difficult task & it cannot be conducted in a quantitative manner.

32. Write short notes on Info System Maintenance.What are the different types of maintenance? Nov 2008, 2010, 2011

Ans. Most info systems require some modification after development due to failure to anticipate all requirements during system design and changing organizational requirements. The process of enhancing the existing system according to the changed requirements is called system maintenance.

Types of System Maintenance

1. **Scheduled Maintenance** - It can be anticipated & planned for.
   Example - Implementation of new inventory coding scheme can be planned in advance.
2. **Rescue Maintenance** - It refers to previously undetected errors that were not anticipated but require immediate solution.
3. **Corrective Maintenance** - It deals with fixing bugs in the code or defects found.The need for corrective maintenance is usually initiated by bug reports drawn up by the end users.
   Example - (i) Correcting a failure to test for all possible conditions **or**
   (ii) Correcting a failure to process the last record in a file.
4. **Adaptive Maintenance [RTP May 2014]** - It consists of adapting software to changes in the environment, such as Hardware or Operating System. The need for adaptive maintenance can only be recognised by monitoring the environment.
5. **Perfective Maintenance** - (i) It mainly deals with accommodating to new or changed user requirements and
   (ii) concerns functional enhancements to the system & activities to increase the system's performance or to enhance its user interface.
6. **Preventive Maintenance** - The long term effect of corrective, adaptive & perfective changes and continuous changes in program increases the system's complexity, which is required to be reduced.The process by which, system's complexity is reduced is called preventive maintenance.

33. Write short notes on Operation Manual.

Ans. It refers to a user's guide or a technical communication document intended to give assistance to system users.It is usually written by a technical writer who may be programmers,project managers or other technical staff.These are most commonly associated with electronic goods,computer hardware & software.

Operation manual includes the following:

i. Cover page,Title page and Copyright page;
ii. Preface - containing details of related documents & info on how to navigate the user guide;
iii. Contents page;
iv. Guide on how to use at least the main functions of the system;
v. Troubleshooting section - detailing possible errors or problems that may occur, along with how to fix them;
vi. FAQs (Frequently asked questions) ;
vii. Where to find further help & contact details;
viii. Glossary & Index (for larger documents).

34. Write short notes on System Development Team.Also explain their roles involved in SDLC. Nov 11, RTP May 14

Ans. People responsible for system development & their roles in SDLC are typically explained below:

1. **Steering Committee** - This committee consists of a group of key info system service users that acts as a review body for info system plans & applications development

Role: (i) Responsible for all costs & timetables (ii) Provide directions & ensures appropriate representation of affected parties. (iii) Conducting regular review of progress of the project.(iv) Taking corrective actions like re-scheduling, re-staffing,re-designing etc.

2. **Project Manager** - A project manager is normally responsible for :
(i) Delivery of project within time & budget (ii) Periodical reviews of project's progress with the project leader & his team.
(iii) Liaisons (means communication & co-operation) with the client.

3. **Project Leader** - He is responsible for completion of a project & fulfillment of objectives.He reviews the project's progress more frequently than the project manager and the entire project team reports to him.

4. **System Analyst/Business Analyst** - His main responsibility is to conduct interviews with users & understand their requirements. He is a link b/w users & programmers who converts the user requirements in the system requirements and plays an important role in the requirement analysis & design phase.

5. **Module Leader/Team Leader** - Since a project is divided into several manageable modules,so the development responsibility for each module is assigned to module leaders.They are responsible for delivery of tested modules within stipulated time & cost.

6. **Programmer/Coder/Developer** - He is responsible to convert design into programs using programming language.He also tested the program for debugging activity.

7. **Database Administrator (DBA)** - The DBA handles multiple projects;ensures the integrity & security of info stored in database and also helps the application development team in database performance issues.

8. **Tester** - He is a junior level quality assurance personnel attached to a project who tests programs & sub-programs as per the plan given by the module/project leaders and prepares test reports.

9. **Domain Specialist** - He helps the project team to develop applications in new fields.**For example:** If a project team undertakes application development in insurance,about which they have only a little knowledge,they may seek the assistance of an insurance expert at different stages.

10. **IS Auditor** - He ensures that the application development also focuses on the control perspective.He should be involved at Design Phase & final Testing Phase to ensure the existence & operations of the controls in new software.

11. **Accountant** - An Accountant has knowledge in IT, Business, Accounting, Internal Controls, Behavior & communications etc that can be applied in development efforts.In addition, he can also perform Economic Feasibility/Cost-Benefit analysis to choose an optimum solution.

35. Explain the objectives of "Audit of Systems under development" in the context of SDLC.

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

1. To provide an opinion on the Efficiency,Effectiveness, and Economy of project mgt.
2. To assess the extent to which the system being developed provides for adequate audit trails & controls to ensure the integrity of data processed & stored; and
3. To assess the controls being provided for the management of the system's operation.

CHAPTER 3 - CONTROL OBJECTIVES

1. What do you mean by Controls? Why is there a Need for controls in an IT environment?

Controls: Controls can be defined as: policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented or detected and corrected.

Need for Controls:

1. High Cost of Data Loss: Data is a critical resource of an organization & if it is lost then it can result in huge financial loss to the organization.

2. Incorrect Decision Making: If IT environment is not equipped with proper controls then slight deviation in any process can give wrong information which can result in wrong decision making by the end user of that information.

3. Costs of Computer Abuse: Unauthorized access to computer systems, computer viruses, unauthorized physical access to computer facilities and unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, documentation etc.)

4. Value of Computer Hardware, Software and Personnel: These are critical and expensive resources of an organization and have huge impact on business competitiveness.

5. High Costs of Computer Error: In a computerized environment a single data error during entry or processing can cause great damage.

6. Maintenance of Privacy: Today data collected in a business process contains personal info about an individual or customer like medical, educational, employment, residence etc. If this information gets leaked then the organization will face severe consequences.

7. Controlled evolution of computer Use: Technology use and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

2. Briefly explain the Objectives of the information systems audit.

Information Systems auditing is the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively and uses resources efficiently.

1. Asset Safeguarding Objectives: The IT assets (hardware, software, data files etc.) must be protected by a system of internal controls from unauthorized access and misuse.

2. Data Integrity Objectives: Data integrity means that organizations data does not undergo any unauthorized modification, deletion or addition.

3. System Effectiveness Objectives: Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet substantial user requirements.

4. System Efficiency Objectives: Efficiency means to optimize the use of various information system resources (machine time, peripherals devices, system/application software and labour) in best possible manner.

5. Compliance: To ensure Compliance with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

3. Discuss the effect/impact of Computers on Internal Controls.

The major areas of impact are as follows –

(1) Personnel : We need to check whether or not staffs are trustworthy; whether they have the appropriate skills and training to carry out their jobs or not.

(2) Segregation of duties : Segregation basically means to see that one person cannot process a transaction through from start to finish. However, in a computerized system, the auditor should also be concerned with the segregation of duties between the departments and within the IT department.

(3) Authorization procedure : In some online transaction systems, written evidence of individual data entry authorization may be replaced by computerized authorization controls such as user name and password.

(4) Record keeping : Automated controls will be required to protect the storage of documents, transaction details, and audit trails as they are in machine readable form.

(5) Access to assets & records : In the manual systems, assets could be protected from unauthorized access through the use of locked doors and filing cabinets. In the computerized systems, computer programs and data are vulnerable to unauthorized amendment from remote locations. The use of wide area networks, including the internet, has also increased the risk of unauthorized access.The nature and types of control available have changed, to address these new risks.

(6) Management supervision : Increased management's supervision & review helps to deter and detect both errors and fraud.

(7) Concentration of programs & data : Transaction and master file data (e.g. pay rates, approved suppliers lists, etc.) may be stored in a computer readable form on one computer and computer programs such as file editors are likely to be stored in the same location as the data. Therefore, in the absence of appropriate controls over these programs and utilities, there is an increased risk of unauthorized access to, and alteration of financial data.

4. XYZ ltd is a large multinational company with offices in many locations. It stores all its data in just one centralized computer centre. It uses internal controls in order to Asset Safeguarding, Data Integrity, System Efficiency & Effectiveness. What could be inter-related components of its internal controls? Discuss them briefly. Nov 2012

Internal controls used within an organisation comprise of the following five interrelated components:

1. Control Environment: Management's policy and procedure, organization hierarchy and the ways authority and responsibility are assigned makes the control environment. This element implements controls in the CBIS.

2. Risk Assessment: It is the elements that identify & analyze the risks faced by an organisation & the ways the risk can be managed.

3. Control Activities: This element operates to ensure that transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance occur. These are called Accounting controls.

4. Info and Communication: It is the element, in which info is identified, captured & exchanged in a timely & appropriate form.
5. Monitoring: This element ensure that internal controls operate reliably over time.

5. Briefly explain the Effect of computers on Internal Audit.

The move towards more automated financial systems has the following impact in the way auditors carry out their work -

1. Changes in the Evidence Collection:

Audit trail is the key requirement in financial audit. Automated systems have made the following changes in audit trail and evidences.

(i) Data retention and storage:

♦ A client's storage capabilities may restrict the amount of historical data that can be retained on-line & readily accessible to the auditor. If the client has insufficient data retention capacities, then the auditor may not be able to review a whole reporting period's transactions.

♦ If the client uses a computerized financial system all or part of the audit trail may only exist in machine readable form. It can not be understood by the auditor what the Is and Os mean. The data must be translated into normal text by an additional process before it can be read and understood by the auditor.

♦ When a client gives the auditor a magnetic disk containing transaction details and data has been uploaded onto the auditor's machine, special audit software may be required to interrogate the information.

(ii) Absence of input document: In many accounting system transaction data may be entered into the computer directly without the presence of supporting document. The increasing use of EDI will result in less paperwork being available for audit examination.

(iii) Lack of visible audit trail: The audit trails in some computer systems may exist for only a short period of time. It calls 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.

(iv) Lack of visible output: In many systems processing may not produce a hard copy form of output, that makes it necessary for the auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a terminal and being granted "read" access to the required data files.

(v) Audit evidence of automated transaction: Certain transactions may be generated automatically by the computer system. ***For e.g***. A fixed asset system may automatically calculate depreciation on assets. Where transactions are system generated, the process of formal transaction authorization may not have been explicitly provided in the same way as in a manual environment. This may alter the risk that transaction may be irregular.

(vi) Legal issues: More and more organizations 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, what are the terms of the contract and the parties to the contract. The laws regarding computer evidence varies state to state, country to country & even court to court. If the auditor intends to gather evidence for use in a court, he should firstly find out what the local or national laws stipulate on the subject.

2. Changes in Evidence Evaluation:

(i) System generated transactions: Computerized financial systems may have the ability to initiate, approve and record financial transactions. Clients are starting to use these types of systems because they can increase processing efficiency & there will be no need to employ someone to do it manually.

Automated transaction generation system are frequently used in inventory control system when a stock level falls below re-order level, the system automatically generates a purchase order and sends it to the supplier.

Automated transaction processing systems can cause the auditor problems. The auditor may need to look at the application's programming to determine whether the programmed levels of authority (internal control) are appropriate.

(ii) Systematic Error: Computers are designed to carry out processing on a consistent basis. If the computer is doing the right thing, then with all other things being equal, it will continue to do right thing every time. Similarly, if the computer is doing the wrong thing or processing a transaction incorrectly, it will continue to handle the same type of transactions incorrectly, every time. Therefore, whenever an auditor finds an error in a computer processed transaction, he should be thorough in determining the underlying reason for the error. If the error is due to a systematic problem, the computer may have processed hundreds or more of similar transactions incorrectly.

6. "Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems". Explain briefly management's responsibility for establishing controls.

Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems. Therefore, management must take systematic and proactive approach to do the following -

1. Long range planning: The elements of long-range planning incorporate -

(i) Goals & objectives of the plan-for use in measuring progress, (iii) Time allowance and target date
(ii) Revenue and expense estimates. (iv) Strengths and weakness

2. Long -range planning and IT department: The IS manager must take systematic and proactive measures to -

(i) Develop & implement appropriate, cost-effective internal control structure (iv) Identify needed improvements;
(ii) Assess the adequacy of internal control (v) Take corresponding corrective action; and
(iii) Assess internal control to check their adherence to the IS policy of the organisation. (vi) Report annually on internal control

3. Short-range planning or Tactical Planning: The management is also responsible to develop plan for the functions and activities performed every day to meet the long range goals.

For example: Data processing job plan that defines daily processing activities.

4. Personnel Management controls: The management is responsible to develop plan to accomplish the administration of individuals. ***The control technique are-***

(i) **Job descriptions:** It's a mgt control to communicate mgt requirements & provide a standard for performance mgt.
(ii) **Salary and benefits budget:** To identify the cost factors & evolve a strategic plan for new products & services.
(iii) **Recruiting standards and criteria:** This control is critical for defining recruitment criteria for various IS positions which requires technical training & experience to develop & maintain operational efficiency.
(iv) **Job performance evaluations:** To counsel & motivate employees to maintain system quality & to meet deadlines & budget time.

(v) **Screening and security standards:** To prevent anyone of security concern from gaining access to IS assets etc.

Important Note: ***Topics related to IS Audit are covered in Chapter 9.***

7. "Implementing & operating controls in a system involves costs". Explain these costs.

(i) Initial Setup Cost: This cost is incurred to design and implement controls. ***For example -*** A security specialist must be employed to design a physical security system.

(ii) Executing cost: This cost is associated with the execution of a control.

For example - The cost incurred in using a processor to execute input validation routines for a security system.

(iii) Correction Cost: The control has operated reliably in signaling an error or irregularity, the cost associated with the correction of error or irregularity.

(iv) Failure cost: The control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses.

(v) Maintenance cost: The cost associated in ensuring the correct working of a control. ***For example*** - Rewriting input validation routines as the format of input data changes.

♦ Internal control benefits can be seen in the form of Reduced losses. One way to calculate benefits involves expected loss i.e. mathematical product of risk and exposure. Here benefits of a control procedure is the difference between the expected loss with the control procedure and the expected loss without it.

♦ After estimating benefits and costs, management determines whether the control structure is cost-effective or not.

♦ In evaluating cost/benefit of control procedure, mgt must consider factors other than those in the expected benefit calculation.

For e.g. - If an exposure threatens an organization's existence, it may be worthwhile to spend more then indicated by the cost-benefit analysis.

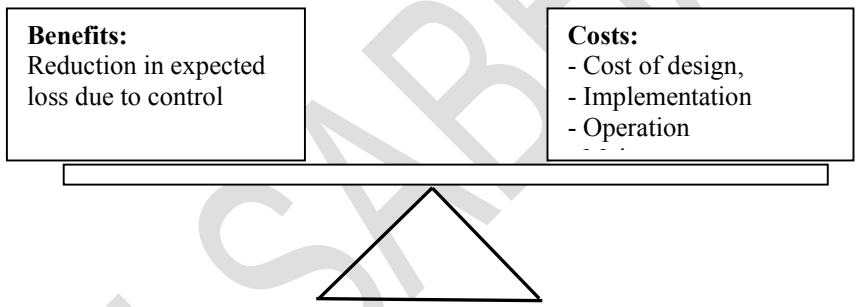
8. Briefly explain the viability/cost-effectiveness of internal Cost Control Procedures.

Internal controls are essential element in any business process but they have two problems which should be taken care of:

1st– Controls involve cost.

2nd– Controls make the process slow.

Thus, Cost effectiveness of controls means benefits of an internal control must exceed its cost. Since too many controls can negatively affect operational efficiency, therefore, the objective of designing internal control system is to provide reasonable assurance that control problems do not take place.



COST BENEFIT-ANALYSIS OF CONTROL

Costs are easier to measure than benefits because most of the control benefits are intangible. After estimating benefits & costs, mgt determines whether the control is cost effective or not.

Example - At one MNC, data errors occasionally required the entire payroll to be re-processed at a cost of Rs. 10,000.Mgt determined that a data validation step would reduce error risk from 15% to 1% at a cost of Rs. 600/pay period.The time taken for validation causes an additional cost of Rs. 100. **RTP May 2009; June 2009 (Similar)**

Sol. Computation of Net Expected Benefit of Validation Procedure -

Particulars	Without Validation Procedure	With Validation Procedure	Net Expected Difference
a) Cost of reprocess entire payroll	Rs. 10,000	Rs. 10,000	
b) Risk of payroll data errors	15%	1%	
c) Expected reprocessing cost (a) x (b)	Rs. 1,500	Rs. 100	Rs. 1,400
d) Cost of validation procedure	Nil	(600+100) = Rs. 700	Rs. (700)
e) Net expected benefit of validation procedure			Rs. 700

% of net benefit to gross benefit, i.e effectiveness = (e) / (c) x 100 = 700/1400 * 100 = 50%

Conclusion: The proposal is worthwhile.

9. What do you mean by Control Objectives?

Control objective is defined as "A statement of the purpose to be achieved by implementing control procedures in IT process". The statement of controls serve two main purposes:

1. Outline the policies of the organization as laid down by the management.
2. A benchmark for evaluating whether control objectives are met.

The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss. **Some categories of exposures are :**

(i) Errors or omissions

(vi) Weak general control

(ii) Improper authorizations and improper accountability
(iii) Inefficient activity in processing
(iv) Lack of management understanding of IS risks
(v) Absence or inadequate IS control framework
(vii) Lack awareness and knowledge of IS risk
(viii) Distributed computing environments
(ix) Inappropriate technology implementations

10. Briefly explain the various Categories of Controls.

(A) Classification of Controls on the basis of Objectives:

We put controls into 4 categories depending on the objectives of control -

(i) Preventive Controls:

Suggest preventive control measures to avoid errors for improvement. June 2009

What do you mean by Preventive Controls? Discuss with the help of examples. Also explain broad characteristics of these controls. RTP May 2014

Preventative controls are those which are designed to prevent an error, omission or malicious act that may occur in financial system. **Some of the preventive controls are** -

(i) Employ qualified personnel
(ii) Login procedure
(iii) Documentation
(iv) Authorization of transaction
(v) Firewalls
(vi) Segregation of duties
(vii) Access privilege control
(viii) Training of staff
(ix) Data validation controls
(x) Anti-virus software

Broad Characteristics of Preventive Controls are as under: (Or, For implementing preventive controls knowledge of the following is required)

1. A clear-cut understanding about the vulnerabilities of the asset.
2. Understanding probable threats.
3. Provision of necessary controls for probable threats from materializing.

(ii) Detective Controls:

What do you mean by Detective Controls? Explain with the help of examples. RTP May 2012

These controls are designed to detect error, omission or malicious acts that occur in the system and report the occurrence. **The main characteristics of these controls are** -

1. It require clear understanding of lawful activities so that anything which deviates from these is reported.
2. It require an established mechanism to refer the reported unlawful activities to the appropriate person.
3. It interacts with the preventive control to prevent such acts in future.
4. It ensures surprise checks by supervisor.

Some of the Detective controls are -

(i) Hash total
(ii) Echo check
(iii) The internal audit functions
(iv) Bank reconciliation
(v) Check points during processing
(vi) Duplicate checking of calculations
(vii) Intrusion detection system
(viii) Monitoring expenditures against budgeted amount

(iii) Corrective Controls:

What do you understand by corrective controls? Discuss with the help of examples. Also explain the main characteristics of these controls. RTP Nov 2012, RTP Nov 2013

Corrective controls are designed to reduce the impact of an error or correct an error, once it has been detected. **The main characteristics of these controls are** -

1. They minimizes the impact of the threat.
2. They help in identifying the cause of the problem.
3. They resolve the problem discovered by detective controls.
4. They get feedback from preventive and detective controls
5. They correct error arising from a problem

Some of the Corrective controls are -

(i) Contingency planning
(ii) Rerun procedure
(iii) Investigate budget variance and report violations
(iv) Backup procedure
(v) Change input value to an application systems

(iv) Compensatory Controls:

While designing the appropriate control one thing should be kept in mind that the cost of the lock should not be more than the cost of the asset it protects. Sometimes while designing and implementing controls, organizations may not be able to implement appropriate controls because of different constraints such as financial, administrative or operational. In such a scenario, there should be adequate compensatory measure which may although not be as efficient as the appropriate control, should be implemented. These controls are basically designed to reduce the probability of threat that causes a loss to an asset.

(B) Classification of Controls on the basis of nature of IS resources:

Another classification of controls is based on the nature of such controls with regard to the nature of resource to which they are applied -

(i) Environmental controls: Controls relating to Power, AC , UPS,Smoke detection, Fire-extinguishers, de-humidifiers etc.

(ii) Physical Access controls : Controls relating to physical security of the IS resources 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 OS controls, Application software controls, Networking controls, Encryption controls etc.

(iv) IS Operational Controls : Controls relating to IS operation and administration such as Timing controls, IS infrastructure management, Help desk operations etc.

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

(vi) SDLC Controls: Controls relating to planning, design, development, testing, implementation & post implementation, change mgt.

(C) Classification of Controls on the basis of Functional Nature:

"While reviewing a client's control system, an IS auditor will identify three components of Internal Controls." State & briefly explain these three components. June 2009

The basic purpose of IS controls in an organization is to ensure that the business objectives are achieved & undesired risk events are prevented or detected and corrected. This is achieved by designing an effective info control framework. While reviewing a client's control system, an IS auditor will be able to identify three components of internal controls. Each component is aimed at achieving different objectives as stated below:

(i) Accounting controls : Controls to safeguard the client's assets and to ensure the reliability of the financial records.

(ii) Operational controls : These controls deals with the day to day operations to ensure that the operational activities are contributing to business objectives.

(iii) Administrative controls: These controls are concerned with ensuring efficiency and compliance with management policies.

11. Briefly explain the various Information system Control Techniques.

Control Techniques: The basic purpose of IS controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing control framework, which comprise policies, procedures, practices and organization structure that gives reasonable assurance that the business objectives will be achieved.

Various control techniques are as follows:

1. Organizational Controls :- These controls are concerned with decision-making processes that lead to mgt authorization of transactions. Organizational control techniques include the followings -

(i) Responsibilities and objectives: Each IS function must be clearly defined & documented, including systems software, application programming & systems development, database administration and operations. The IS mgt team is responsible for the effective & efficient utilization of IS resources, so they set the objectives to be achieved and responsibilities of resource utilization.

Their responsibilities include:

(a) Providing information to senior management on the IS resources (b) Planning for expansion of IS resources
(c) Implementing activities that support companies strategic plan (d) Controlling the use of IS resources

(ii) Policies, Standards, Procedures and Practices: These are the standards and instructions that all IS personnel must follow when completing their assigned duties. Policies establish the rules delegated to individuals in the enterprise. Procedures establish the instructions that individuals must follow to compete their daily assigned tasks. Documented policies should exist in IS for:

(a) Use of IS resources, (b) Physical security, (c) Data security
(d) On-line security, (e) Microcomputer use, (f) System development methodology

(iii) Job descriptions: These communicate management's expectations for job performance.It provides instructions on how to do the job. All jobs must have a current, documented job description readily available to the employee. It establishes responsibility & the accountability.

(iv) Segregation of duties: It is aimed at separating conflicting job duties to discourage fraud. Such separation can also force an accuracy check of one-person work by another. ***Examples of segregation of duties are :***

♦ Systems software programming from the application programming
♦ Database administration from other data processing activities
♦ Application programming group into various subgroups for individual application systems

From a functional perspective, segregation of duties should be maintained between the following functions:

(a) Information systems use (b) Computer operation (c) Data entry
(d) System administration (e) Security administration

2. Management Controls: The controls adopted by the management to ensure that the information systems functions correctly and meet the strategic business objectives. The scope of control includes framing IT policies, procedures and standards on a holistic view. ***The controls to consider when reviewing management controls in an IS system shall include:***

(i) Responsibility : The strategy to have a senior management personnel responsible for the IS within the organisational structure.

(ii) An official IT structure : There should be a prescribed organisation structure with clear roles and responsibilities through written and agreed job descriptions.

(iii) An IT steering committee : The steering committee shall comprise of user representatives from all areas of the business, management representative & IT personnel.

3. Financial Control: These controls are exercised by the system user personnel over source of transactions and documents before system input. The financial control techniques are numerous. ***A few examples are highlighted here:***

i) Authorization: i.e obtaining the authority to perform some act.

ii) Budgets: These are the estimates of the amount of time or money expected to be spent during a particular period of time, project, or event.

iii) Cancellation of documents: This is a typical control over invoices marked with a "paid" or "processed" stamp or punching a hole in the document to prevent its reuse..

iv) Documentation: This includes written instructions to explain how to perform the task and also written explanations of actual task performed.

v) Dual control: This entails having two people simultaneously access an asset. For example, the filling of money in ATM should be performed by two people present.

vi) I/O verification: This entails comparing the information provided by a computer system to the input documents.

vii) Safekeeping: This entails physically securing assets under lock and key.

viii) Segregation of duties: This entails assigning similar functions to separate people to provide reasonable assurance against fraud and provide an accuracy check.

ix) Sequentially numbered documents: These are working documents with preprinted sequential numbers, which enables the detection of missing documents.

x) Supervisory review: This control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them.

4. Data processing Environment Controls: These controls are hardware and software related and exercised in the IS environmental areas that include system software programming, on-line programming, database administration, media library, application program change control etc.

5. Physical Access Controls: These controls are exercised on access to IT resources by employees/outsiders. These Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to authorized individuals. IT management should ensure a low profile is kept and the physical identification of the site of the IT operations is limited. The other measures relate to Visitor Escort, Personnel Health and Safety, Protection against environmental Factors and Un-interruptible Power Supply.

6. Logical Access Controls: These controls are software related controls used to ensure that access to systems, data and programs is restricted to authorized users. The key factors in designing logical access controls include authorization, authentication and access control, user identification and authorization profiles, incident handling, reporting and followup, virus prevention and detection, firewalls user training and intrusion testing and reporting etc.

7. SDLC (System Development Life Cycle) controls: These are functions that control the development of application systems. The first control is system development standards that specify the activities that should occur in each system development life cycle (SDLC) phase. Second control is the standards that specify the type and quantity of testing that should be conducted. The third element of controls is documented procedures.

8. Business Continuity (BCP) Controls: These controls relate to having an operational and tested IT continuity plan. The controls include criticality classification, alternative procedures, backup and recovery, systematic and regular testing and training, monitoring and fallback and resumption plans, risk management activities, assessment of single point of failure.

9. Application Control Techniques: These include the programmatic routines within the application program code to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls include form design, source document controls, input, processing and output controls, media identification, data back-up and recovery.

10. Audit Trails:

As an IS Auditor, explain how audit trails can be used to support security objectives? May 2010

Audit trails are logs that can be designed to record activities at the system, application, and user level. It is an important detective control to help accomplish security policy objectives. Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirement, detect the consequences of error and allow system monitoring and tuning.

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

(i) **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact, to protect the system from outsiders who are attempting to breach system controls. Depending upon how much activity is being logged and reviewed, real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

(ii) **Reconstructing Events :** Audit analysis can be used to reconstruct the steps that led to event 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 avoid similar situations in the future. The audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

(iii) **Personal Accountability :** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior, if they know that their actions are recorded in an audit log.

Implementing an Audit Trail:

The information contained in audit logs is useful in measuring the potential damage associated with application errors, abuse of authority, or unauthorized access by outside intruders. Logs also provide valuable evidence on both the adequacies of controls and the need for additional controls. Audit logs, however, can generate data in overwhelming detail, thus, poorly designed logs can actually be dysfunctional.

12. Briefly explain the User Controls to be exercised for system efficiency & effectiveness.

A counter clerk at a bank is required to perform various business activities as part of his j ob description and assigned responsibilities. He is able to relate to the advantages of technology when he is able to interact with the computer system from the perspective of meeting his job objectives. The following user controls are exercised for system effectiveness and efficiency:

1. Boundary Controls:

What Boundary Control Techniques should be used in user controls? RTP May 2012, May 2013

The major controls of the boundary system are the access control mechanisms. Access controls are implemented with an access control mechanism & links the authentic users to the authorized resources which they are permitted to access. The access control mechanism has the three steps of identification, authentication & authorization with respect to the access control policy.

Boundary control techniques are as follows:

(i) Cryptography: It involves transforming data into codes that are meaning less to anyone who does not possess the authentication to access the respective data/file. The three techniques of cryptography are Transposition, Substitution and product cipher (combination of transposition and substitution).
(ii) Passwords: User identification by 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. The best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.
(iii) Personal Identification Numbers (PIN): It is similar to a password assigned to a user by an institution. PIN is vulnerable to exposed while issuance, delivery, transmit or store.
(iv) Identification Cards: These are used to store information required in an authentication process.
2. Input Controls: These are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important since input of data, involve human intervention and are therefore error and fraud prone. Poorly designed data codes cause recording and keying errors.

Briefly explain the various Types of Data Coding Errors. Also explain the factors affecting these errors.

Types of data coding errors are as follows:
(i) Addition : Addition of an extra character in a code e.g. 54329 coded as 543219
(ii) Truncation : Omission of characters in the code e.g. 54329 coded as 5439
(iii) Transcription: Recording wrong characters 54329 coded as 55329
(iv) Transposition: Reversing adjacent characters 54329 coded as 45329
(v) Double transposition: Reversing characters separated by one or more characters i.e. 54329 is coded as 52349
Factors affecting coding errors are as follows:
(i) Length of the code: Long codes are naturally prone to more errors therefore they should be broken using hyphens, slashes or spaces to reduce coding errors.
(ii) Alphabetic numeric mix: The code should provide for grouping of alphabets and numerical separate if both are used. Intermingling both would result in more errors.
(iii) Choice of characters: Certain alphabets are confused with numerical such as B, 1,0, S, V and Z would be confused with 8,1,0,5,U, 2. Such characters should be avoided.
(iv) Mixing uppercase / lowercase fonts : Upper case and lower case should NOT be mixed when using codes since they delay the process of keying in due to usage of the shift key.
(v) Sequence of characters: Character sequence should be maintained as much as possible. Such as using ABC instead of ACB. Control used to guard against these types of errors is a ***"Check Digit"***. Check digits are redundant digits that helps verify the accuracy of other characters in the code that is checked. The program recalculates the check digits & compares with the check digit in the code when the code is entered to verify If the code is correct. Check digits may be prefixes or suffixes to the actual data.
3. Processing Controls:

What are the data processing controls? Briefly explain the various data processing controls.

Processing Controls: Data processing controls perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. Normally the processing controls are enforced through the DBMS, however, adequate controls should be enforced through the front end application system also to have consistency in the control process. ***Data processing controls are:***
♦ **Run-to-Run totals:**
♦ **Reasonableness verification:**T wo or more fields can be cross verified to ensure their correctness.
♦ **Edit check:** The data validation controls to verify accuracy and completeness of data.
♦ **Field initialization:**Setting all values to zero before.
♦ **Exception Reports:** Exception reports are generated to identify errors in data processed. Such exception reports give the transaction code and reason why the particular transaction was not processed.
♦ **Existence/Recovery Controls:** The check point/Restart logs facility is a short-term backup and recovery control that enables a system to be recovered if failure is temporary and localized.
4. Output Controls:

What is the Scope of Output Controls of an application system? Suggest various types of output controls which are enforced for confidentiality, integrity & consistency of output. May 2013

These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. 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 & routed to the users.

Various types of Data Controls which are enforced for confidentiality, integrity & 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.
♦ **Logging of output program execution:** When programs used for output of data are executed, it should be logged and monitored.
♦ **Spooling/Queuing:** When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is sent to the printer as soon as the printer is read to accept the data. This intermediate storage of output could lead to unauthorized disclosure or modification
♦ **Controls over printing :** 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. Distribution should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A report log should be maintained.
♦ **Retention controls :** Retention controls consider the duration for which outputs should be retained before being destroy.
♦ **Existence/Recovery Controls :** These controls are needed to recover out in the event that it is lost or destroyed. Check point /restart log helps in recovery when a hardware problem causes a program that prints customer invoices to abort in midstream.
5. Database Controls: Protecting the integrity of a database when application software acts as an interface to interact between the user and the database are called database controls. **They are classified into two categories:**
(i) Update Controls:
♦ **Sequence Check Transaction & Master Files:** Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updation, insertion or deletion of records.
♦ **Ensure All Records on Files are Processed:** While processing; the transaction file records check processing upto the end-of-file.
♦ **Process multiple transactions for a single record in the correct order:** Multiple Transactions can occur based on a single master record (e.g. dispatch of a product to different distribution centers).
♦ **Maintain a Suspense Account:** When mapping between the master record to transaction record results in a mismatch then these transactions are maintained in a suspense account.
(ii) Report Controls:
♦ **Standing Data:** Application programs use many internal tables to perform various functions say billing calculation based on a price table. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.
♦ **Print-Run-to-Run control Total:** It helps in identifying errors or irregularities like wrong sequence of updating.
♦ **Print Suspense Account Entries:** Similar to the update controls the suspense account entries are to be periodically monitors with the respective error file and action taken on time.
♦ **Existence/Recovery Controls:** The back-up and recovery strategies required to restore failure in a database. Recover strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) method.

13. Write short note on 'key elements in System Development and Acquisition Control'. Nov 2008

It is important to have a formal, appropriate, and proven methodology to govern the development, acquisition, implementation, and maintenance of information systems. Methodology should contain appropriate controls for management review and approval, user involvement, analysis, design, testing, implementation, and conversion. Many institutes have provided framework that help organizations to design their control structure. **Some of them are :**
(i) Acquire and Implement-7 (AI7),
(ii) Control Objectives for Information and related Technology (COBIT),
(iii) Capability Maturity Model (CMM),
(iv) IT Infrastructure Library (ITIL),
(v) ISO/IEC 17799 , and
(vi) COSO

14. As an IS auditor, how will you examine the controls that are important in the major System Development Phases?

The following subsections will examine the controls that are important in the major system development phases:
1. Problem definition: In this phase, the stakeholders must attempt to come to an understanding of the nature of the problem or opportunity which they are addressing.

Controls	IS Auditor's Role
• Need for IS in the view of business objectives • Support and priority for the IS by the management. • Level of acceptance among the stakeholders on the need for change. • Investigate to justify the need for the system.	• Check whether the stakeholders have reached an agreement on the existence of a problem. • Understand the threats to asset safeguarding, data integrity, system effectiveness & system efficiency associated with the solutions proposed for the system.

2. Management of the Change Process: This process runs parallel to all phases of SDLC.

Controls	IS Auditor's Role
Change-facilitation deals with the following critical activities – • Preparing the organization for change by feedback, training, participatory decision making and promote the need for change. • Complete change over to the new system. • To help users adapt to their new roles. • Project mgt involves addressing matters such as Budgeting, Exception reporting, Checkpoints & User coordination.	• To evaluate the quality of procedure of change facilitation. • Suggest that change management can be done in-house, if the proposed system is small and has a localized impact on users. • If the proposed system is large and has high-levels of requirements and technological uncertainty then determine the effect on organization structures and jobs.

3. Entry and feasibility assessment: The specific techniques used to evaluate the feasibility of systems depend on the type and size of the system being proposed.

Controls	IS Auditor's Role
• **Technical Feasibility:** Can technology be acquired, developed or available to support the proposed project? • **Operational Feasibility:** Can the system be designed to process inputs and give required outputs? • **Economic Feasibility:** The proposed system is deemed feasible only if the benefits exceed all the cost requirements. • **Behavioral Feasibility:** Can the system improve the quality of	• Determine that the change proposed is not imposed upon stakeholders. • Determine the behavioral impact on the users and the problems that arise. • Determine the material losses incurred as result of the development, implementation, operation or maintenance of the system.

work life of the users?	

4. Analysis of the existing system: To design a new system, it is essential to understand the existing system. An analysis should include
• A study of the organizational history of the system.
• A study of the existing information flows.

Controls	IS Auditor's Role
1. The study of system's history gives an idea of the types of systems that have been extremely useful; issues that have not been addressed over a period; and new issues that require attention. 2. The study of existing info flows is done using formal methodologies like top-down structured analysis (waterfall), prototyping, & agile models to understand the system.	• Study the aspects of the present organizational structure, history & culture. • Study the context in which the decisions for the new proposed system choice was made and its implications for the conduct of the audit. • Evaluate the quality of methodologies used. • Analyze the usage of high-quality tools in analysis and documentation.

5. Formulation of strategic Requirements (System Design): The strategic requirements also called as the SRS document.

Controls	IS Auditor's Role
• Align the business requirements with the management's objectives and user's goals. • Elicitation of the requirements and system-design work concurrently.	• Evaluate the quality of the SRS design work. • Evaluate the feasibility of the system-design proposed. • Assess the identified procedures and substantial behavioral impact on the users.

6. Organizational and job design: Adapting the organizational structures and job responsibility with respect to the proposed system often leads to behavioral problems among its stakeholders and may result in implementation failure.

Controls	IS Auditor's Role
• The roles and responsibilities of users of the system are to be defined using formal traditional mechanism. • A clear design of the responsibilities in the initial design phase is critical in achieving the goals.	• Assess the assigned responsibility and process used to resolve conflicts. • Assess the control risk associated with the responsibilities during SDLC with substantive testing.

7. Information Processing Systems Design: From efficiency viewpoint, the reliability of the controls designed into the system are to be evaluated to meet the strategic requirements of the proposed system.

Controls	IS Auditor's Role
• Requirements elicitation: Interview, GDs, Prototyping. • User interface design: Source document, Screen layout, Report formats, Icons. • Data/Information flow design: DFD. • Database design: Conceptual modeling, data modeling, physical layout. • Plat form design: H/w and S/W design, modularity, generality. • Physical Design: Identify boundaries, Modules, Packages and Programs.	• To evaluate the appropriateness of the requirements-elicitation strategy. • To evaluate 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. • To evaluate the design and quality of the interface that needs to follow best design practices.

8. Application Software Acquisition/Selection Process: Once the information processing is identified and designed then the application software may be acquired or developed in-house. **RTP Nov 2013**

Controls	IS Auditor's Role
• Info & system requirements need to meet business & system goals. • A feasibility analysis to define the constraints or limitations for each alternative system from a technical as well as a business perspective. • A detailed Request for Proposal (RFP) document needs to specify the acceptable requirements (functional, technical, & contractual). • 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 me supplier application, - Customized modifications of the application software.	• To ensure that the decision to acquire software should flow from the thorough feasibility study, vendor evaluation and RFP adequacy checked for. • A RFP would include transaction volume, data base size, turnaround time & response time requirements & vendor responsibilities. • Check the criteria for pre-qualification of vendors & sufficient documentation available to justify the selection of the final vendor. • The auditor may also collect information through his own sources on vendor viability, support infrastructure, Service record. • Review the contract signed with the vendor for adequacy of safeguards & completeness. The contract should address the contingency plan in case of vendor failures. • To ensure that the contract went through legal scrutiny before it was signed.

15. Briefly explain the various Controls over System and Program changes.

1. Management of the change process: The complexity of hardware, software, and application relationships in the operating environment needs well defined, planned, coordinated, tested, and implemented change management. Mgt of the change process runs parallel to all the phases of SDLC.

The change process involves the following tasks:

(i) Provide feedback to the system stakeholders (iv) Helps users to adapt to new roles

(ii) Prevents system disruptions (v) Documentation of the implemented process changes.
(iii) Accept changeover to a new system across the organization

2. System Change Controls: (Refer Q.No. 20 for Controls & IS Auditor's Role)

"The Change Control Processes deal with some risks". Explain these risks.

The Change Control process of a system under development is to address the problems not detected during system design or testing. A change control evaluation includes checks on problems reporting, tracking; prioritizing, and resolving. The risks the change control processes deal with are:

(i) System outages due to error, omissions, or malicious intent, (iv) Fraud / abuse to company systems and data,
(ii) Data loss or errors due to error, omissions, or malicious intent, (v) Repeated errors, and
(iii) Unauthorized changes, (vi) Reruns of system or application processes.

The objective of a change management review are to ensure that changes made to the system and programs do not adversely affect system, application, or data.

3. Program Change Controls:

♦ Implementing controls over the modification of application software programs is to ensure that only authorized programs and modifications are implemented.

♦ Failure of proper controls leads to risks in software security like threats deliberately omitted or turned off processing irregularities or malicious code.

Auditor's Role in Program Change Controls is given below:

(i) Ensure appropriate backups of the system's data and programs made before the change.
(ii) Tracking of program changes are to be accounted for through version procedure.
(iii) A formal handover process so that authorized personnel are involved in the software changes.
(iv) Standardized software updation management policies, procedures, & tools;
(v) A thorough testing, before any new software release is applied in production environment.

4. Authorization Controls: These controls ensure that all information and data entered or used in processing is authorized management and representatives of events that actually occurred.

Describe the auditor's role in Authorization Controls. RTP Nov 2013

Auditor's Role in Authorization Controls is given below:

(i) Transactions in an application system are manually authorized, the controls that ensure that no authorized modifications take place after authorization.
(ii) If transaction authorization is facilitated by logical access restrictions, then verify if the appropriate people have these capabilities.
(iii) Identify any allowable overrides or bypasses of data validation & edit checks and determine who can do the overrides.
(iv) Make sure that there is an audit trail for all urgent matters.
(v) Review by IT management to monitor, and approve all changes to hardware, software, and personnel responsibilities.
(vi) Assigned and authorized responsibilities to those involved in the change.

5. Document Controls:

Documentation contains descriptions of the hardware, software, policies standards, procedures, and approvals related to the system. **A user instruction manual document defines:**

♦ Input controls that identify all data entering the processing cycle;
♦ Processing control information that includes edits, error handling, audit trails and master file changes;
♦ Output controls that define how to verify the correctness of the reports;
♦ Separation of duties between preparing the input and balancing the output.

To provide the user with the tools to achieve their responsibilities, the user manual should include:

(i) A narrative description of the system (iv) A copy of each input document, completed as an example
(ii) A detailed flowchart of all clerical processes. (v) A list of approvals required on each input document
(iii) A detailed document flowchart.

Auditor's Role in Document Controls:

Assessing documentation involves evaluating -

(i) There is sufficient documentation that explains how software/hardware is to be used.
(ii) There are formal, documented security and operational procedures.
(iii) The auditor will need to obtain documents with the following details:

a) Name (title) of the computer product f) Point of origin for each source document
b) Purpose of the product g) Destination of each copy of the source document
c) Date the system was implemented h) Each operating unit or office through which data is processed
d) Type of computer used and location i) Actions taken by each unit or office in which the data is processed
e) Frequency of processing and type of processing

6. Testing and Quality Control: Testing commences during the design phase and continues during the system development and acceptance testing phases. Computer system are tested to prove that they perform to the satisfaction of the various interested parties. This includes the developers, operations staff, and the end-users and may also include system administrators, security personnel and auditors.

♦ The overall objective of the testing process is to ensure that the delivered system is of adequate quality. To meet this objective it will be necessary to confirm that the new system:-

(i) conforms with the organization's technical policies and standards; (iv) meets it performance objectives;
(ii) performs all me required functions; (v) is reliable in operation.

(iii) can be used by the staff for whom it is intended;
♦ Tests must therefore be designed to demonstrate that the system:
- does not do what it is supposed to do;
- does what it is not supposed to do;
- is not operable by the staff for whom it is intended.

♦ Other important principle that should govern testing are -
(i) No testing without measurable objective (iii) No recording without analysis
(ii) No testing without recording (iv) No analysis without action

16. Define the term "Regression Testing".

Defects uncovered during testing might be corrected if they are considered to be significant to justify the cost & time involved in taking remedial action. But, it may be preferable to live with a defect, if it is trivial, or defer remedial action until a more convenient time. If a defect is corrected, the system (or perhaps parts of it) will probably need to be re-tested to ensure that the change has not introduced other unforeseen problems. This process is known as "regression testing".

17. Write short notes on Quality Control.

Quality control is concerned with the quality of individual product produced during the project, it is the responsibility of the Project Manager to ensure that effective quality control is carried out. It costs both time and money, and project manager are often tempted to dispense with it, particularly when working to an unrealistic, imposed deadline. Quality control management is a process that impacts the effectiveness, efficiency, integrity, and availability of information systems. Quality controls encompass the following:
(i) Establishment of a quality culture (vi) Program and system testing and documentation
(ii) Quality plans (vii) Quality assurance reviews and reporting
(iii) Quality assurance responsibilities (viii) Training and involvement of end-user and quality assurance personnel
(iv) Quality control practices (ix) Development of a quality assurance knowledge base
(v) System development life cycle methodology (x) Benchmarking against industry norms
This control requires regular reviews and audits of the software products and activities to verify that process and personal comply with the applicable procedures and standards.

18. Write short notes on Quality Standards.

The best practices that identify the quality and assurance are governed by two key standards.:
i) Capability Maturity Model integration (CMM): Developed by Software Engineering Institute SEI); it is a framework for organizing and assessing the maturity level of IT processes for software development and maintenance.
ii) 9000 Quality Management and Quality Assurance Standards (ISO): Defines quality control as the "operational techniques and activities that are used to fulfill requirements for quality".

19. Write short notes on Quality Reviews.

Quality review covers various non-computer testing activities. For example, it determines whether a product is:
❖ Complete and free from cosmetic and mechanical defect.
❖ Is correct, comprehensive and appropriately targeted.
❖ Complies with relevant standard.

20. As an IS Auditor, what general questions will you consider for Quality Control? RTP May 2012, RTP May 2013

The general questions that the auditor will need to consider for quality control are:
(i) Does the system design follow a defined and acceptable standard?
(ii) Are completed designs discussed and agreed with the users?
(iii) Does the project's quality assurance procedures ensure that project documentation is reviewed against the technical standards and policies and the User Requirements Specification;
(iv) Do quality reviews follow a defined and acceptable standard?
(v) Are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;
(vi) Are auditors/security staffs invited to comment on the internal control aspects of system designs
(vii) Are statistics of defects uncovered during quality reviews analyzed for trends?
(viii) Are defects uncovered during quality reviews always corrected?
(ix) Has a System Installation Plan been developed and quality reviewed?
(x) Has a Training Plan been developed and quality reviewed?

21. Write short notes on Copyright Violations. Also, explain the Scope of Copyright Act.

Software programs can easily be copied or installed on multiple computers, this is called in ***"Piracy"***. Violation of copyright laws may lead to potential risk. Therefore, computing environment needs controlling to prevent software piracy & copyright violations.
The Scope of a Copyright Act is:
(i) The illegal copy of computer programs except for backup or archival purposes.
(ii) Any business or individual convicted of illegally copying software is liable for both compensatory and statutory damages for each illegal copy of software in the premises.
(iii) Employees and consultants about organizations that use illegal software are documented.
The Copyright Notice: Any info owned/created by the company & considered its intellectual property in a written, printed, or stored as data, must be labeled with a copyright notice in the format like : Copyright ©[Company Name], Inc. All Rights Reserved.

22. Define Contract / Warranties related to IT. Also explain the areas of IT-related contracts to be reviewed by IS Auditors.

On Acquisition of Software systems, organizations enter into contracts for computer hardware, software, and services.

IT contracts are to address these issues:
- Meet IT users expectations and the systems need to perform as intended;
- Able to file litigation in response to dissatisfaction with products or services.

IT auditors can help companies avoid contract failures, especially those lacking in-house computer contracting expertise in areas as *First time purchases, Contract services for computer maintenance, Custom applications, and Multiple supplier procurements.*

The review areas of IT related contracts are -

(i) Review of supplier contract terms that limit supplier liability.
(ii) Review of performance measurements to ensure objectives have been met.
(iii) Review contract clauses for protecting customer interests.
(iv) The three key goals to achieve while contacting for computer goods & services are:
- ♦ Preparation of explicit criteria that can be used for acceptance
- ♦ The process of negotiating the contract and
- ♦ The process of monitoring contract compliance.

(v) To identify a major control weakness and contract issues which require immediate management attention.
(vi) Does the contract reflect the organization's requirement.
(vii) Have the requirements been translated into measurable acceptance criteria?
(viii) Was the contracting officer present at all meetings and documentation of proceedings recorded?
(ix) What changes or agreements were reached in refining contract terms?
(x) Acceptance tests are documented, evaluated, and the results are reviewed and signed off by customers.

23. Write short notes on Service Level Agreement (SLA).

The SLA is a formal agreement b/w a customer requiring services & the organization responsible for providing those services. It is not a legal contract in itself, but an essential component of it. An SLA states the required performance of the system in terms of its availability to users, response times, & numbers of transactions processed and any other suitable criteria meaningful to the user.

Service : A set of deliverables that asses between a provider & a consumer.
Level : The measurement of services agreed and delivered and the gap between the two.
Agreement: Contract between two entities - one who is providing the service and other who is receiving the service.

An SLA should also define:
- The level of technical support to be provided to users.
- The procedures for proposing change to the system.
- Standards of security provision, data access controls, monitoring system and network use.
- Emergency requirements; and
- A schedule of charges for the services to be provided.

24. Explain the IS Auditor's role relating to Service Level Agreement (SLA).

The auditor is to ensure that the following form a part of the service level agreement:
- Service provider should comply with all legal requirements that are applicable to the outsourced activity.
- Should provide for a right to audit clause and control responsibilities.
- Responsibility of the service provider to establish performance monitoring procedures.
- Business continuity measures to be put in place to ensure continuity of service.
- Non disclosure requirements as regards information and processes of the audited organization Insurance requirements.

25. Briefly explain the various activities during the implementation stage.

Activities during Implementation stage are discussed below -

1. Procedures Development: Covers who, what, when, where, and how of the implementation process. The design of procedures must match the job/task responsibility of a user within the organizational functional framework.

The auditor is to assess the following in the procedure document design phase:
- The quality of the procedures design must meet the minimum user requirements.
- Change management principles implemented and followed within the organization.
- The approach followed in testing and implementation.
- Quality of the procedures documentation, system manuals etc, in a consistent and formal style.

2. Conversion:

Briefly describe various activities involved in a conversion process during system implementation. Also explain different strategies used in a conversion process. RTP May 2012

It involves the following activities:
(i) Defines the procedures for correcting and converting data into the new application, determining what data can be converted through software and what data manually.
(ii) Performing data standardization before data conversion.
(iii) Identifying the methods to access the accuracy of conversion like record counts & control total,
(iv) Designing exception reports showing the data which could not be converted.
(v) Establishing responsibility for verifying and signing off and accepting overall conversion

The conversion strategies are: (Refer Q.No.29 From Chapter 2)
♦ Direct implementation/Abrupt change-over:
♦ Parallel implementation: Phased implementation: Pilot implementation:

Explain the role of IS Auditor in Data Conversion.

The IS Auditor will determine the following :

(i) Has a data conversion plan been drawn up?
(ii) Does the Data Conversion Plan:
a) Describe the data conversion strategy to be followed ?
b) Allocate staff to each task and define specific roles and responsibilities.
c) Set out the criteria for identifying and resolving problems on the quality of the existing data
d) Acceptance tests using any custom built software.
e) Define procedures to ensure that converted data is kept up-to-date following its transfer to the new system?
f) Define, backup and recovery procedures for the converted data on the new system
g) Define how the audit trail is to be preserved after cut over.

3. User Final Acceptance Testing: Acceptance testing is a complete end-to-end test of the operational system. Appointing an experienced manager and following-up a pre-defined plan will help to ensure that testing is effective. It aims to provide the system users with confirmation that -

♦ The user requirement specification has been mat.
♦ End-user & operational documentation is accurate,comprehensive & usable.
♦ Supporting clerical procedures work effectively.
♦ Help Desk and other support functions operate correctly and as expected.
♦ Backup and Recovery procedures work effectively.

Types of Acceptance Testing: Acceptance test plan involves:

i) Performance Testing: It should address -

♦ **Average Response Time:** i.e. the time b/w user depressing the transmit key & the first character of reply appearing on screen.
♦ **Maximum Response Time:** i.e. the response time that must not be exceeded.
♦ **Other Response Time:** ***For e.g.*** the time to -

❖ Load an application
❖ Accept or move between fields on the screen
❖ Perform a single or multiple update
❖ Run a complex query

ii) Volume Testing: Testing whether the system can handle the volume of data specified in a acceptable time-frame.
iii) Stress Testing: Testing whether the system can handle heavy stress i.e. peak volume of data over a short period.
iv) Security testing: Testing the internal controls and systems security against attempts to upset the security protection.
v) Clerical procedure checking: Testing to confirm that all supporting clerical procedures have been documented and work effectively.
vi) Backup and Recovery Testing: Testing to confirm that software, configuration files, data and transaction logs can be backed up, either completely or selectively and also restored from backup.

Explain the role of IS Auditor in User Final Acceptance Testing.

The auditor is to assure management that both developers & users have thoroughly tested the system to ensure that the system:
(i) Meets the needs of the user and management;
(ii) Provides the capability to support audit of the system in operation;
(iii) Has an Acceptance Test Plan been drawn up to cover all aspects of testing?
(iv) Fully involve the end-users in the design and execution of the acceptance testing programme?
(v) Include ancillary procedures?
(vi) Have test data been prepared for each test?
(vii) Does user Acceptance Testing Plan cover all aspects of the User Requirements?
(viii) Are regression tests carried out to ensure that previously accepted areas of the new system continue to work after significant changes have been implemented?
(ix) Has the acceptance-testing programme been signed off by the Project Board on successful completion?
(x) If the level of testing does not meet standards, the auditor must notify the development team or management who will then take corrective action.

4. User training: Training both the end-users and the IS operations personnel is critical for the efficient and effective implementation of a system. Training would involve manager's training on overview and application of systems, operational user training on how to use the software, enter the data, and generate the output and systems training on the technical aspects.

26. Write short notes on System Maintenance Phase during the implementation of system.

System maintenance is an important phase during the implementation of system. If so, what are the three categories in which maintenance can be undertaken? As an IS auditor of the organization, how will you evaluate the effectiveness & efficiency of the system? Nov 2010

It is an important phase during system implementation.The maintenance phase involves making changes to hardware, software, and documentation to support its operational effectiveness. It includes making changes to improve a system's performance, correct problems, enhance security, or address user requirements.

System maintenance can be undertaken in the following **three categories:**

(i) Corrective maintenance: Emergency error fixing and routine debugging logical errors.
(ii) Adaptive maintenance: Accommodations of changes in the user environment.
(iii) Perfective maintenance: User enhancements, improved documentation, and re-coding.

Auditor's Role in System Maintenance:

Describe the metrics used for the evaluation of effectiveness & efficiency of the system maintenance. RTP May 2013

The effectiveness and efficiency of the system maintenance process is evaluated by auditor using following parameters:
• The ratio of actual maintenance cost per application versus the average of all applications. Avg. time to deliver change requests.
• The number of change requests for the system application that were related to bugs.

• The number of production problems per application and per respective maintenance changes.
• The instances of divergence from std. procedures such as undocumented applications, unapproved design, & testing reductions.
• The quantity of modules returned to development due to errors discovered in acceptance testing.
• Time elapsed to analyze and fix problems.

27. What are the factors for measurement metric under Performance Measurement?

Performance measurement is dependent on the business strategy and objectives of the organization. The factors for measurement metric would involve:

♦ The value delivered by the IT system;
♦ The ratio to the cost of IT to the per unit business function;
♦ The response time of the system for a new or change in operation,and
♦ The ongoing costs of the system to maintain its effectiveness.

For a system to be evaluated properly, it must be assessed using system performance measurement Common measurements include throughput, Utilization used and response time.

28. What is the significance of Post Implementation Review? How is it performed? Nov 2011

After the development project is completed, a PIR should be reviewed to determine whether the anticipated benefits are achieved or not. The PIR should be reviewed jointly by the project development team and the appropriate end users; or alternatively an independent group (internal or external; and not associated with the development process) should carry out the audit, to meet the following objectives:

1. Business Objective: Developed within budgeted cost and time; producing predicted results.
2. User Objective: User friendliness; response time; work load; required output; reliability.
3.Technical Objective: Modularity; ease of operation and maintain; interface with other system.
Timing i.e when should PIR be performed:

♦ PIR should not be undertaken until any changes & tuning that are necessary to achieve a stable system have not been completed.
♦ Sufficient time should also be allowed for the system's user to become familiar with it.
♦ These criteria should be met between 6 and 12 months after implementation. If PIR is delayed beyond 12 months there will be an increasing risk of changing requirement -loading to further release of the system.

29. Write short notes on the PIR Team.

(i) Independent Team: In order to achieve impartial outcome, the team should be substantially independent of the original system development team. It may therefore be advisable to employ an external IS consultant to review.
(ii) External Support: It may also be necessary to employ other external support to assist in evaluating the technical and specialized function of the system.
(iii) Internal Assistance: Internal auditor might help assess the effectiveness of internal controls.

30. What are the activities to be undertaken during PIR? Nov 2012

The team should review -

1. The main functionality of the operational system against the User requirement specification.
2. System performance and operations
3. Development techniques and methodology employed
4. Estimated time-scales & budget and reason for variation, if any.
5. The findings, conclusions & recommendations in a report for the authorizing authority to consider
6. All anticipated benefits both tangible and intangible, delivered by the system.
7. All unanticipated benefits both tangible & intangible, delivered by the system.

31. What are the issues that should be considered by system Auditor at PIR stage before preparing the audit report?
What are the issues to be considered by an IS auditor while judging the effectiveness of PIR? June 2009

The following issues should be considered when judging the effectiveness of a PIR or to form basis for auditing [Or, an auditor will consider following issues at PIR (Post implementation Review) stage before preparing the audit report]:

(i) Interview business users in each functional area covered by the system, & assess their satisfaction with the system.
(ii) Interview security, operations and maintenance staff & assess their reactions to the system.
(iii) Determine whether the system's requirements have been met; If not, then identify the reasons why any requirements are not to be provided, are yet to be delivered, or which do not work properly.
(iv) Review system problem reports and change proposals to establish the no. & nature of problems.
(v) Confirm that adequate internal controls have been built into the system
(vi) Confirm that an adequate Service Level Agreement has been drawn up and implemented
(vii) Confirm that the system is being backed up in accordance with user requirements
(viii) Review the Business Case to determine whether the anticipated benefits have been achieved.

32. What do you mean by Classification of Information? Explain different classification of information. Nov 2008

Information classification is the decision to assign a level of sensitivity to information. This classification of the information should then determine the extent to which it needs to be controlled or protected. It is also indicative of its value in terms of business assets. ***Broadly information is classified into 5 categories*** -

Information Classification	Description of Information	Examples	Security Level
Top Secret	(i) Highly sensitive internal info. (ii) Restricted distribution of info	Investment strategies, Pending mergers or acquisitions	Highest possible
Highly Confidential	information that, if made public or even shared around the organization could seriously obstruct the	Accounting info, business plans, sensitive customer's data, suppliers data etc.	Very high

	organization's operations.		
Proprietary	Information is of a proprietary nature so made available to authorized personnel only.	Procedures, operational work routine, project plans, designs & specifications etc.	High
Internal Use only	It includes information not approved for general circulation outside the organization. The loss/disclosure of these informations would cause inconvenience to the organization but not result in financial loss or serious damage.	Internal memo, minutes of meetings, project reports etc.	Controlled but normal
Public Documents	Info which has been approved for public use.	Annual reports, press statement etc	Minimal

33. "Once the information is classified on various levels, the organization has to decide about the implementation of different Data Integrity Controls." Do you agree? If yes, explain about data integrity & its policies. Nov 2010

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

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

Data Integrity Policies

♦ **Virus-Signature Updating:** Virus signatures must be updated immediately when they are made available from the vendor.

♦ **Software Testing:** All s/w must be tested in a suitable test environment before installation on production system.

♦ **Division of Environment:** Division of environment into development, test, & production is required for critical systems.

♦ **Version Zero Software:** Version zero s/w (1.0, 2.0 & so on) must be avoided whenever possible to avoid undiscovered bugs.

♦ **Offsite Backup Storage :** Backups older than one month must be sent offsite for permanent storage.

♦ **Quarter-End and Year-End Backups :** These backups must be done separately from the normal schedule for accounting purposes.

♦ **Disaster Recovery:** A comprehensive DRP must be used to ensure continuity of the corporate business in the event of an outage.

34. What do you mean by Data Integrity? Explain the six categories of integrity controls.

Data Integrity: once the information is classified, the organization has to decide about various data integrity controls to be implemented. The primary objective of data integrity control techniques is to prevent, detect and correct errors in transactions as they flow through the various stages of a specific data processing program. Data integrity controls protects data from accidental or malicious alteration and provide assurance to the user that the info meets expectations about its quality & integrity.

There are six categories of integrity controls:

Control Category	Threats/Risks	Controls
Source Data Control	Invalid, incomplete, or inaccurate source data input	Good form design, sequentially pre-numbered forms, cancellation & storage of documents etc.
Input Validation Routines	Invalid or inaccurate data in computer-processed transaction files	Edit checks, sequence, validity. Enter exceptions in an error log, prepare a summary error report.
On-line Data Entry Controls	Invalid or inaccurate transaction input entered through on-line terminals	User IDs & p/w, promoting operators during data entry, closed loop verification, transaction log etc.
Data Processing & Storage Controls	Inaccurate or incomplete data in computer processed master files	Monitoring & accelerating data entry by data control personnel, reconciliation of system updates with control A/Cs or reports, exception reporting, data conversion controls
Output Controls	Inaccurate or incomplete computer output	Visual review of computer output, reconciliation of batch totals, proper distribution of output, storing of sensitive output in secure area
Data Transmission Controls	Unauthorized access to transmitted data or to the system itself, system failures, errors in data transmission	Monitoring of network to detect weak points, preventive maintenance, data encryption, routing verification, party checking, message acknowledgment procedures etc.

35. Define Data Security. Explain the IS Auditor's role while reviewing the adequacy of data security controls.

Data security encompasses the protection of data against accidental or intentional disclosure to unauthorized persons. And prevention of unauthorized modification & deletion of data. Many levels of data security are necessary in an IS environment like ***database protection, data integrity, security of h/w & s/w controls, physical security over the user etc.***

The disclosure of sensitive info is a serious concern to the organization and is mandatory on the auditor's list of priorities while reviewing the adequacy of data security controls. An IS auditor is responsible to evaluate the following in this regard:

(i) Who is responsible for the accuracy of the data?

(ii) Who is permitted to update data?

(iii) Who is permitted to read and use the data?

(iv) Who is responsible for determining who can read and update the data?

(v) Who controls the security of the data?

36. What is a Cryptosystem? Nov 2009, RTP Nov 2012, RTP May 2014

A Cryptosystem refers to a set of algorithms needed to implement a particular form of encryption and decryption. Typically, a cryptosystem consists of three algorithms : one for key generation, one for encryption and one for decryption.the term cryptosystems is most often used when the key generation algorithm is important. Cryptosystem is commonly used for symmetric key techniques.

37. Define the term 'Cipher'.

The term **"Cipher"** is used to refer to a pair of algorithms one for encryption and one for decryption. Cipher is also used for symmetric techniques.

38. Write short notes on Data Encryption Standard (DES). Nov 2009, RTP Nov2012, RTP May 2014

❖ The DES is a cipher algorithm selected as an official Federal Information Processing Standard (FTPS) for **USA** in **1976**. It is mathematical algorithm for encrypting and decrypting binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext.

❖ The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key. ***A key consists of 64 binary digits*** of which ***56 bits are randomly generated*** and used directly by the algorithm. The other ***8 bits***, which are not used by the algorithm, ***are used for error detection***. The 8 error detecting bits are set to make the parity of each 8 bits byte of the key odd.

❖ Authorised users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. Unauthorised recipient of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically.

Disadvantage: DES is now considered to be insecure for many applications. This is mainly due to the 56 bit key size being too small; DES keys have been broken in less than 24 hours.

39. Write short notes on Public Key Infrastructure (PKI). Imp.

The system is based on public key cryptography in which each user has a key pair - a unique electronic value called a **public key** and a mathematically related **private key.** The ***pvt. key is stored on the user's computer or a separate device*** such as a smart card. The private key must be stored in encrypted text and protected with a password or PIN to avoid compromise or disclose. The private key is used to create an electronic identifier called a digital signature that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key. It is important when issuing a digital certificate that the initially verifying the identity of users is adequately controlled. The Certifying Authority (CA) attests to the individual user's identity by signing the digital certificate with its own private key, known as the root key. The user's private key exists electronically and is susceptible to being copied over a network as easily as any other electronic file. If it is lost or compromised, the user can no longer be assured that message will remain private or that fraudulent or erroneous transaction would not be performed.

Drawback of a PKI authentication system is that it is more complicated and costly to implement than user names and password.

40. Discuss the policies & controls that any financial institution needs to consider when utilizing PKI. May 2011

When utilizing PKI policies and controls, financial institution need to consider the following -

♦ Defining the methods of initial verification that are appropriate for different types of certificate applicants and controls for issuing digital certificates.

♦ Selecting an appropriate certificate validity period to minimize transactional and reputational risk exposure.

♦ Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions.

♦ Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a user's private key or the closing of user account.

♦ Updating the database of revoked certificates frequently.

♦ Employing measures to protect the root key including limited physical access to certifying authority facilities, tamper-resistant security modules.

♦ Requiring regular independent audit to ensure controls are in place, public and private key lengths remain appropriate, cryptographic module conform to industry standards.

♦ Recording all significant events performed by the CA system in a secure audit log.

♦ Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions & unauthorised activities.

♦ Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require acceptance of the financial institution's certificates by other CA's.

41. Write short notes on Firewall. June 2009, May 2011

A firewall is a collection of components (computers, routers and s/w) that mediate access b/w different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of flow. They are ideally situated to inspect & block traffic and coordinate activities with network intrusion detection systems (IDS).

Typically, firewall block or allow traffic based on the rules configured by the administrator. Rule set can be static or dynamic. A static rule set is an unchanged statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic rule set often is a result of coordinating a firewall and an IDS. **For eg.** An IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address.

Firewalls are subject to failure. When firewalls fall, they should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

42. Briefly explain various Types of Firewalls.

The selection of firewall type is dependent on the amount of traffic, the sensitivity of the system and data, and application.There are 4 primary firewall types from which to choose, these are:

1. Packet Filter firewalls:

What do you mean by Packet Filter Firewall? Explain major weaknesses associated with it. RTP May 12, 13 & 14; M 13

These firewalls ***evaluate the headers of each incoming and outgoing packet*** to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service. **If** the packet does not match the pre-defined policy for allowed traffic, **then** the firewall drops the packet. Packet filter generally do not analyze the packet contents beyond the header info.

Weaknesses associated with packet filtering firewall includes the following:

♦ The system is unable to prevent attacks that exploit application because the packet filter does not examine packet contents.

♦ Logging functionality is limited to the same information used to make access control decision.

♦ Most do not support advanced user authentication schemes
♦ Firewalls are generally vulnerable to attack and exploitation that take advantage of vulnerabilities in network protocols.
♦ Firewalls are easy to mis configure, which allows traffic to pass that should be blocked.
Packet filtering are appropriate in high-speed environment where logging and user authentication with network resources are not as important. Packet filter firewall are also commonly used in small office / home office (SOHO).
2. Stateful inspection Firewalls: These firewalls are packet filters that monitor the state of the TCP connection. Each TCP session starts with an ***initial "handshake"*** communicated through TCP flags in the header information. When a connection is established the firewall adds the connection information to a table. The firewall can then compare future packets to the connections or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.
3. Proxy server firewalls: These firewalls act as ***an intermediary between internal and external IP addresses*** and block direct access to the internal network. ***They rewrite packet headers*** to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capabilities, proxy servers are commonly employed behind other firewall devices. The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate proxy server. ***Common proxy servers are*** Domain Name Server(DNS), Web server(HTTP), and Mail (SMTP) server. Additionally, proxy servers provide another layer of access control by segregating the flow of internet traffic to support additional authentication and logging capability, as well as content filtering.
4. Application-level firewalls:

Discuss Application Level Firewalls along with its primary disadvantages. RTP Nov 2013

These firewalls combine the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or service such as telnet, FTP, HTTP, SMTP etc. These firewalls provide the strongest level of security, but are slower and require greater expertise to administer property.
Disadvantages of Application-level firewalls:
♦ The time required to read and interpret each packet slows network traffic.
♦ It may provide only limited support for new network application and protocols. They may also allow traffic from those applications & protocols to go through the firewall.

43. List some of the additional services provided by firewalls.

Firewalls may provide some additional services, These are:
1. Network address translation(NAT) -NAT re-addresses outbound packets to mask the internal IP addresses of the network. NAT allows an institution to hide the topology and address schemes of its trusted network from un-trusted networks.
2. Dynamic host configured protocol(DHCP) - It assigns IP addresses to machines that will be subject to the security controls of the firewall.
3. Virtual Private Network(VPN) gateway - A VPN gateway provides an encrypted tunnel between a remote external gateway and the internal network. Placing VPN capability on the firewall protects information from disclosure. Firewall are subject to failure. When firewall fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass

44. What do you mean by Unauthorised Intrusion? Why is there need for Intrusion Detection System?

Unauthorized Intrusion: The computer systems of an organization are mostly attached to a network and perhaps even to the internet. And, the organization allows access from the network only to authorized people. But, there may be some persons using the network who can intrude into the system to gain unauthorized access. This is called unauthorized intrusion to a computer system.
For e.g. If there is a web server, attached to the internet, only clients, staff, & potential clients are allowed to access the web pages stored on that web server. It does not allow unauthorized access to that system by staff, customers, or unauthorized third parties.
Intrusion Detection System: Intrusion detection is an attempt to monitor and possibly prevent attempts to intrude into system and network resources of an organization. It is the set of mechanisms that should be put in place to warn of attempted unauthorized access to the computer. IDS can also take some steps to deny access to would-be intruders.
Need for IDS: Computer systems of an organization are generally attached to a network, and sometimes even to the internet. The organizations might use some mechanisms like passwords, file security etc. to prevent unauthorized access to the computer system, which may lead to a range of issues. So, there is a need for permitting access to that computer system from the network, only to the authorized persons. Since, simple password or authentication system can be broken in some cases, Therefore, there is a need for adequate system security to protect data.
Types of IDS: IDS fall into two broad categories. These are -
1. Network based system - These types of systems are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries.
2. Host based system - These types of IDS runs on the system being monitored. These examine the system to determine whether the activity on the system is acceptable.

45. Write short notes on 'Hacking'. How the hackers are different from crackers. Imp.

Hacking: It is an act of penetrating computer systems to gain knowledge about the system and how it works.

Hacker	Cracker
A hacker is someone who is enthusiastic about computer programming.What damage can a hacker do depends upon what backdoor program(s) are holding on the PC. Hackers can see everything you are doing, and can access any file on your disk. He can write new file, delete files, edit file, and do practically anything to a file that could be done to a file. A hacker could install several programs on to your system without your	Cracker are people who try to gain unauthorized access to computers.This is normally done through the use of a 'backdoor' program installed on the machine. A lot of cracker also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer. However if a cracker can't do something using the backdoor

knowledge. Such programs could also be used to steal personal information such as password and credit card information.	program, he can easily put something else onto your computer.

46. What do you mean by Unauthorised Intrusion? What is Hacking and what damage can a hacker do? May 2012

Unauthorized Intrusion: (Please refer Q.No. 49)

Hacking: (Please refer Q.No. 50)

The type & degree of damage that a hacker can do to info stored in a computer system depends upon the backdoor program hiding on the PC. Different programs can do different amounts of damage. Typically, Hackers can do following damages to computerized info:

(i) They can smuggle another program onto your PC.

(ii) They can see everything you are doing & can access any file on your disk.

(iii) They can write new files, delete files, edit files, and do practically anything to a file that could be done by a genuine user.

(iv) They could install several programs on to your system without your knowledge.

(v) They can steal personal info such as passwords and credit card info.

47. What is hacking? Explain the ways, which can be used by a hacker for hacking. RTP Nov 2013

Hackers: (Please refer Q.No. 50)

There are many ways in which a hacker can hack. Some are -

(i) NetBIOS: NetBIOS hackers don't require to have any hidden backdoor program running on your computer. NetBIOS is meant to be used on local area networks, so machines on that network can share information.

(ii) ICMP 'Ping'(Internet Control Message Protocol): 'Ping' is one of the commands that can be sent to a computer using ICMP. Ordinarily, a computer would respond to this ping, telling the sender that the computer does exist. Ping may seen harmless enough, but a large number of pings can make a Denial-of-Service attack, which overloads a computer. Hacker can use pings to see if a computer exist and does not have a firewall. If a computer responds to a Ping, then the hacker could launch a more serious form of attack against a computer.

(iii) FTP: It Stands for File Transfer Protocol, it can be used for file downloads from some websites. FTP normally requires some form of authentication for access to private files, or for writing to files. FTP backdoor programs such as Doly Trojan, Fore, blade runner etc. simply turn your computer into an FTP server, without any authentication.

(iv) RPC statd: This creates a ***problem of infamous unchecked buffer overflow*** which is specific to Linux and Unix. The problem is where a fixed amount of memory is set aside for storage of data. If data received larger than this buffer, the program should truncate the data or send back an error or atleast do something other than ignore the problem. Unfortunately, the data overflows the memory that has been allocated to it, and the data is written into parts of memory it shouldn't be in. This can cause crashes of various different kinds. A skilled hacker could write bits of program code into memory that may be executed to perform the hacker's evil deeds.

(v) HTTP: It stands for Hypertext Transfer Protocol. HTTP hackers can only be harmful if you are using Microsoft web server software such as Personal Web Server. If a user makes a request for a file on the web server with a very long name, part of the request gets written into that parts of memory that contain active program code. A malicious user could use this to run any program they want on the server.

48. Explain the IS Auditor's Role in the context of Confidentiality, Integrity & Availability (CIA Triad).

The focus of IS Auditor is to examine all factors that adversely bear on the CIA of the info, due to improper physical access. CIA are the core principles of information safety. ***Confidentiality***-Preventing disclosure of information to unauthorised individuals. ***Integrity*** -Preventing modification of data by unauthorised personnel. ***Availability*** -Info must be available when it is needed.

49. What is Data Privacy? Explain the major techniques that are used to address privacy protection for IT systems. Nov 2011, RTP May 2013

It refers to the evolving relationship between technology and the legal right to public expectations of privacy in the collection and sharing of data. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data that are affected by data privacy issues are :

(i) Health information (ii) Criminal justice (iii) Financial information

(iv) Genetic information (v) Location information

Privacy protection for IT systems: In heterogeneous info systems with different privacy rules are interconnected, technical control and logging mechanisms will be required to reconcile,enforce & monitor privacy policy rules and to ensure accountability for info use.There are several technologies to address privacy protection IT systems. ***These fall into two categories -***

(a) Policy communication

P3P- The platform for privacy preferences, P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

(b) Policy Enforcement

XACML - The extensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy.

EPAL -The Enterprise Privacy Authorization Language is very similar to XACML but is not yet a standard.

WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services.

50. What should be the Data Privacy Policies?

1. Copyright Notice: All information owned by the company and considered intellectual property, whether written, printed or stored as data, must be labeled with a copyright notice in a format like - copyright ©[Company Name], Inc. All Rights Reserved.

2. E-mail monitoring: *All e-mails must be monitored for:* Non-business use, unethical or illegal content disclosure of company's confidential information.

3. Customer Information Sharing: Corporate customer info may not be shared with outside companies or individuals.

4. Encryption of data backups: All data backups must be encrypted.
5. Encryption of Extranet Connection: All extranet connections must use encryption to protect the privacy of the info traversing the network.
6. Data Access: Access to corporate information, hard copy, and electronic data must be restricted to individuals with a need to know for a legitimate business reason. Each individual must be granted access only to those corporate info resources which is necessary for them to perform their job functions.

Control against viruses and other destructive programs

Destructive programs are responsible for huge amount of losses measured in terms of data corruption and destruction, degraded computer performance, hardware destructive, violations of privacy.

51. What is a Virus? What policy and procedure controls can be recommended for ensuring control over virus proliferation and damage? May 2012

Virus: A virus is a program that attaches itself to a legitimate program to penetrate the operating system. The virus destroys application programs, data files, & operating systems in a no. of ways. One of the most insidious aspect of a virus is its ability to spread throughout the system and to other systems before perpetrating its destructive acts. When a virus-infected program is executed, the virus searches the system for uninfected programs & copies itself into these programs.
Virus programs usually attach themselves to the following types of files -
1. An .EXE or .COM program file
2. The boot sector of a disk
3. The .OVL program file
4. A device driver program

Recommended policy and procedure control

The policy & procedure controls that can be recommended for ensuring control over virus proliferation & damage are given as follows:
(i) The security policy should address the virus threat, systems vulnerabilities and controls. A separate section on anti-virus is appropriate to address the various degree of risks and suitable controls thereof.
(ii) Anti-virus awareness & training on symptoms of attacks, methods of reducing damage, cleaning should be given to all employees.
(iii) Hardware installations and associated computing devices should be periodically verified for parameter settings.
(iv) As part of SDLC controls, the development area should be free of viruses and sufficient safeguards must be in place to secure area from viruses.
(v) Provision of disk drivers to read media should be restricted to certain controlled terminals and should be write-protected.
(vi) Access to the internet should be restricted preferably to stand-alone computers.
(vii) Networks should be protected by means of firewall that can prevent entry of known viruses.
(viii) The server and all terminals must have rated anti-virus software installed.
(ix) Procedure should ensure that systematic updates are applied to all anti-virus installations.
(x) External media such as disks, CDs, tapes need to be avoided. If necessary such media should be scanned on a stand-alone machine and certified by the department.
(xi) Vendors and consultants should not be allowed to run their demonstration and presentation on organization systems.
(xii) An effective backup plan must be implemented & monitored to ensure that back-up media is not infected & preferably encrypted.

52. Discuss Anti-virus software and its types. Nov 2009, RTP Nov 2012

Among the counter measures against virus attacks, anti-virus software are most widely used techniques to detect viruses, and prevent their further harm.There are three types of anti-virus software -
1. Scanner: The software looks for a sequence of bits called virus signatures that are characteristics of virus codes. They check memory, disk boot sectors, executables and systems filling to find matching bit patterns. It is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.
2. Active Monitor and Heuristic Scanner: This looks for critical interrupt calls such as OS calls & BIOS calls, which resemble virus action. ***However*** this also makes them inefficient since they cannot differentiate b/w genuine systems calls and virus action.
3. Integrity checkers: These can detect any unauthorised changes to files on the system. They require the software to compute a binary check data called the Cyclic Redundancy Check(RCR) for each file. When a program is called for execution, the software computes the CRC again and check with the parameter stored on the disk. Such checks assume that frequent changes to applications and systems utilities do not occur.
However, there is no single control, which can act as a panacea for all virus attacks. Virus control is in fact combination of management, technical, administrative, application & operational controls. The best policy for virus control is preventive control.

53. What critical procedures are to be evaluated while assessing Logical Access Controls?

Logical access controls are used to designate who or what is to have access to a specific system resource and the type of transactions & functions that are permitted. Assessing logical access controls involves evaluating the following critical procedures:
(i) There are logical controls over network access.
(ii) Logical access controls restrict users to authorized transactions and functions.
(iii) There are controls implemented to protect the integrity of the application & the confidence of the public when the public accesses the system.

54. Which are the Logical access paths? What controls are required to different logical access paths?

Following are some logical access paths to the system and the controls that can restrict them to be used by authorised users only -
1. On-line Terminals -It is the terminal, directly connected by server and used by end user. To access an on-line terminal a user has to provide a valid login-ID and password.
2. Operator Console -It is the terminal connected to the server and used by authorised operator only. Access to operator console must be restricted by -
♦ Keeping the operator console at a place, which is visible,at all.
♦ Keeping the operator console in a protected room accessible to selected personnel.

3. Batch job Processing -In a batch processing jobs are accumulated and sent as batches. Thus during an accumulation there is possibility of an unknown job entering into a batch. To avoid this access should be granted to authorised people.

4. Dial-up ports - Using a dial up port user at one location can connect remotely to another computer (unknown location) via a telecommunication media. Security is achieved by providing a means of identifying the remote user to determine authorization to access. A dial back line can also be used to ensures security by confirming the presence of authorised user and data.

5. Telecommunication Network -In a telecommunication network a number of computer terminals, PCs etc are linked to the computer through network. Security is provided in the same manner as it is applied to on-line terminal.

55. Write short notes on Logical Access Issues and Exposures.

Controls that reduce the risk of misuse, theft, alteration or destruction should be used to protect unauthorized & unnecessary access to computer files. Access control mechanism should be applied not only to computer operators but also to end user, programmers, security administrators, management or any other authorised user. Access control mechanism should protect the followings -

(i)Access control software (vi) Logging files
(ii) Application software (vii) Temporary disk files
(iii) System Software (viii) Data Dictionary
(iv) Tape files (ix) Password Library
(v) Data files (x) Telecommunication lines

56. Explain the different types of Technical Exposures in relation to Logical Access.

Intentional or accidental exposure of logical access control encourage technical risks and crimes; of which technical exposures are -

1. Data Diddling: It involves the change of data before or as they entered into the system. A little technical knowledge is required to data diddling and the worst part of it is that it occurs before computer security can protect data.

2. Bombs: Bomb is a piece of a program code deliberated planted in the system. It explode when the condition of explosion get fulfilled, causing the damage. These program does not infect other programs. Generally they are of two kinds -

- **Time bomb:** It causes destructive activities on a particular date and time. The computer clock initiates it.
- **Logic Bomb** -Logic bombs are activated by some occurrence of events.

***For example*:** A code like - if a file named **DELETENOT** is deleted, then destroy the memory contents by writing Is.

3. **Trojan horse [RTP May 2014]:** These are malicious programs that are ***hidden under any authorised program***. They cannot copy themselves to other software in the same or other system. The Trojan may get activated only if the infected program is called explicitly.

A Trojan may -

♦ Change or steal the password ♦ May modify records in protected files ♦ May allow unauthorised user to use the system

4. Worms: A worm does not require a host program like Trojan and it can copy itself to another machine on the network. Since worms are stand-alone program they can be detected easily.

5. Rounding Down: This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorised account. As the amount is small it gets rarely noticed.

6. Salami Technique: In the Salami technique, a very small amount of money is truncated from a computerized transaction.

For example: The amount 21,23,456.39 is truncated to either 21,23,456.30 or 21,23,456.00 depending on the calculation.

7. Trap Doors: These are the back doors that exists in an authorised program and allow to enter into a system without asking for login-ID and password.

57. Explain the Effect of Computer Crime Exposures.

Computer systems may be used to steal money, goods, software or corporate info.Crimes are also committed when false data or unauthorized transaction is made. The crimes that are committed using computers & causes damage to the reputation, morale & very existence of an organization are called computer crimes. Computer crimes generally result in loss of customers, embarrassment to mgt, & legal actions against the organizations.The effects of computer crimes on the organization are:

1. Financial Loss: Financial losses may be direct like loss of electronic funds or indirect like false bills of expenditure.

2. Legal Repercussions: An organization has to adhere to many human rights laws while developing security policies and procedures. The organization will be exposed to lawsuit from investors and insurers if there are no proper security measures.

3. Loss of Credibility: In order to maintain competitive edge, many companies, especially service firms needs credibility and public trusts. This credibility will be shattered resulting in loss of business and prestige if any security violation occurs.

4. Blackmail Espionage: By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.

5. Disclosure of information: Exposure of confidential, sensitive or embarrassing information to the outside world can spoil the reputation of the organization.

6. Sabotage: People who may not be interested in financial gain but who want to spoil the credibility of the company will involve in such activities. They do it because of their dislike toward the organization.

58. Who may be the potential Logical Access Violators?

Logical access violators are often the same people who exploit physical exposures, although the skills required to exploit logical exposures are more technical & complex. The potential logical access violators may be:

(i) Hackers, (ii) Crackers , (iii) Employees, (iv) Former employees, (v) Temporary personnel
(vi) IS Personnel, (vii) End users, (viii) Vendors & consultants , (ix) Competitors, (x) Interested or educated outsiders,
(xi) Criminals , (xii) Foreigners, and (xiii) Accidental ignorant.

59. What is Spoofing?

Spoofing: A spoofing attack involves forging one's source address. Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that he is interacting with the operating system.

For example, a penetrator duplicate the logon procedure, captures the user's password.

60. What are Asynchronous Attacks? Explain the various types of Asynchronous Attacks? RTP Nov 2012

These attacks occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmission must wait for the clearance of the line before data being transmitted. Data that are waiting to be transmitted are liable to unauthorised access called asynchronous attack. These attacks are hard to detect and has many forms:-

1. Data Leakage: It involves leaking information out of the computer by means of dumping files or reports on paper, tapes or disks.

2. Wire Tapping: This involves spying on information being transmitted over telecommunication network.

3. Piggybacking: This is the act of following an authorised person through a secured door or electronically attaching to an authorised telecommunication link. A special terminal is placed into the communication for this purpose.

4. Shut down of computer/Denial of Service: This is initiated through terminals that are directly or indirectly connected to the computer. Individuals who know the high-level systems logon-ID initiate shutting down process. Hackers use this technique to shut down computer system over the internet.

61. Explain the possible ways for controlling the remote & distributed data processing applications. RTP May 13 & 14

Remote & distributed applications can be controlled in many ways. These are -

(i) Physical security can be provided by having the terminal lock when not in use.

(ii) Applications that can be remotely accessed should be logically protected.

(iii) Terminals at remote locations should be monitored carefully for violations.

(iv) There should be proper control mechanisms over system documentation and manuals.

(v) Data transmission over remote locations should be controlled. The sender should attach needed control information that helps the receiving station to verify the genuineness.

(vi) When replicated files exist at multiple locations it must be ensured that all are updated regularly.

62. What critical procedures should be evaluated while assessing the Physical & Environmental Protection?

Physical security & environmental security are the measures taken to protect systems, buildings, & related supporting infrastructures against threats associated with their physical environment. Assessing physical & environmental protection involves evaluating the following critical procedures:

- Adequate physical security controls have been implemented and are commensurate with the risks of physical damage or access.
- Data is protected from interception.
- Mobile & portable systems are protected.

Discuss 'Physical and Environmental Security with Control & Objectives' w.r.t IS policy. [Topic of chapter-8] Nov 09

Designing a secure physical environment to prevent unauthorized access, damage & interference to business premises and info is usually the beginning point of any security plan. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities.

Maintenance of physical operating environment in a computer room is essential. Supporting equipment should be properly maintained. Managing physical controls is ***however*** a difficult task but a good physical security can be very effective.

The detailed control and objectives thereof are as follows:

♦ **Secure Areas:** To prevent unauthorized access, damage and interference to business premises and information.

♦ **Equipment Security:** To prevent loss, damage or compromise of assets and interruption to business activities.

♦ **General Controls:** To prevent compromise or theft of information and information processing facilities.

What are the major points that are required to be taken into consideration for the proper implementation of 'Physical & Environmental Security' with reference to IS Policy? [Topic of chapter 9] Nov 2009, May 2011, RTP Nov 2013

For the proper implementation of Physical and Environment Security, the following points need to taken into account:

(i) Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.

(ii) The IT infrastructure must be physically protected.

(iii) Access to secure areas must remain limited to authorized staff only.

(iv) Confidential and sensitive information and valuable assets must always be securely locked away when not in use.

(v) Computers must never be left unattended while displaying confidential or sensitive information or while logged on to systems.

(vi) Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities

(vii) Equipment, information or software must not be taken off-site without proper authorization.

(viii) Wherever practical, building having computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.

(ix) The location of the equipment/server rooms must not be obvious.

63. Explain the various Logical Access Controls Across the System.

The purpose of logical access controls is to restrict access to information assets/resources. The access should not be so restrictive that it makes the performance of business functions difficult or it should not be so liberal that it can be misused.

The following table shows various categories and the controls in each categories:

Control	(A) User Access Management
1.User Registration	Info about every user is documented, like -Why is the user granted the access? Has the data owner approved Has the user accepted the responsibility? The de-registration process is equally important.
2.Privilege mgt.	Access privileges are to be aligned with job requirements & responsibilities.

3.User Password mgt.	Allocations, storage, revocation, & reissue of password are the password mgt functions.
4. Review of user access rights	A periodic review of access rights is used to check anomalies in the user's current job profile, & the privileges granted earlier.
	(B) User Responsibilities
1. Password use	There must be a mandatory use of strong password to maintain confidentiality.
2.Unattended user equipment	Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password, & should not leave it accessible to others.
	(C) Network Access Control
1. Policy on use of network services	An enterprise-wide applicable internet service requirements should be aligned with the business need policy. Selection of appropriate services & approval tp access them will be part of this policy.
2. Enforced path	Based on risk assessment, it is necessary to specify the exact path/route connecting the networks.
3. Segregation of networks	On the basis of sensitive info handling function, A network for VPN connection b/w head office & branch office is to be isolated from the internet usage service availability for employees.
4.Network connection & routing control	On the basis of identification of source & authentication access policies, The traffic b/w networks should be restricted.
5. Security of network services	This includes the techniques of authentication & authorization policy implemented across the organization's network.
	(D) Operating System Access Control
1. Automated terminal identification	This will help to ensure that, a particular session could only be initiated from a particular location or computer terminal.
2. Terminal Log-On Procedures	The log-on procedure does not provide unnecessary help or info, which could be misused by an intruder.
3. User identification & authentication	Depending on risk assessment, more stringent methods like biometric authentication or cryptographic means like digital certificates should be used.
4. Password mgt system	Internal storage of password should use one-way encryption algorithms & the password file should not be accessible to users.
5. Use of system utilities	Use & access to system utilities should be strictly controlled & logged.
6. Duress alarm to safeguard users	The system should provide a means to alert the authorities which will help to secure the system & system info in case any user executes some instructions under threat.
7. Terminal Time Out	There must be terminal log out time if the user remains inactive for a defined period.
8. Limitation of connection time	Available time slot must be defined which should not allow any transaction beyond the defined time period.
	(E) Application & Monitoring System Access Control
1. Information access restriction	Access to info must be prevented by application specific menu interfaces, so that, the user must be allowed to access only to those items which he is authorized to access.
2. Sensitive system isolation	Based on the critical constitution of a system, it may be necessary to run the system in an isolated environment.
3. Event logging	It is necessary to maintain logs for all types of events in the computer systems.
4. Monitor system use	Based on the risk assessment, a constant monitoring of some critical systems is essential.
5.Clock synchronization	Event logs help in correlating an event & generating a report thereon. Hence, there is a need for synchronizing clock time across the firm.
	(F) Mobile Computing
Mobile Computing	Both physical & logical access to data carried on disk drives of portable computers (Laptop) is critical. So, adequate safeguards like use of encryption & access identification techniques must be used for security.

64. Explain the role of an IS auditor in evaluating Logical Access Controls. May 2010, RTP Nov 2012

An IS auditor should keep the following points in mind while evaluating logical access controls -
(i) Reviewing the relevant document pertaining to logical facilities and risk assessment.
(ii) The potential access paths into the system must be evaluated by the auditor and assess their sufficiency.
(iii) Deficiencies or redundancies must be identified and evaluated.
(iii) By supplying appropriate audit technique, he must be in position to verify controls over access paths.
(iv) He has to evaluate the access control mechanism, analyze the test results and other auditing evidences.
(v) The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.

65. 'Security Policy' - Refer chapter 9 .

66. What are the issues and exposures relating to physical access of computerized systems? Explain the effects of violation of physical access paths.

The following points elucidate the results due to accidental or intentional violations of the access paths:
(i) Abuse of data processing resources
(ii) Blackmail
(iii) Embezzlement
(iv) Damage or theft to equipments or documents
(v) Modification of semester equipment and information
(vi) Public disclosure of sensitive information
(vii) Unauthenticated entry

67. Why is there physical access violation by the employees? Who may be the possible perpetrators?

The possible perpetrators are –

(i) Employees who are Accidental ignorant
(ii) Employee who are Addicted to gambling
(iii) Discontented
(iv) Employees Experiencing financial or emotional problems
(v) Former employee
(vi) Interested or informed outsiders
(vii) Employees notified about their termination
(viii) Employees on strike
(ix) Employees threatened by disciplinary action

68. From an IS Auditor's perspective, list some facilities that need to be protected.

The facilities that need to be protected from the auditor's perspective are:

(i) Communication Circuit (ii) Front end processor (iii) Input/output control room (iv) Micro computer
(v) On-line and remote printers (vi) Programming area (vii) Backup storage facilities (viii) Computer room
(ix) Telephone lines (x) Power sources (xi) Data libraries (xii) Storage room (xiii) LAN

69. Discuss the three processes of Access Control Mechanism, when a user requests for resources. Nov 2009

Access Control Mechanism processes the user request for resources in three steps. They are:

1. Identification 2. Authentication 3. Authorization

Access Control Mechanism operates in the following sequence:

♦ First and foremost, the users have to identify themselves, thereby indicating their intent to request the usage of system resources.
♦ Secondly, the users must authenticate themselves and the mechanism must authenticate itself.
♦ Third, the users request for specific resources, their need for those resources and their areas of usage of these resources.

Identification and Authentication:

Users identify themselves by providing information such as name or account number. To validate the user, his entry is matched with the entry in the authentication file. User may provide 4 classes of authentication information, such as:

Remembered information	Name, account number, password
Object Possessed by the user	Badge number, plastic card key
Personal characteristics	Finger print, Voice print, Signature
Dialog	computer generated information

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

(i) Ticket oriented approach: In this approach, the access control mechanism assigns user a ticket for each resource they are permitted to access. It operates via a row in the matrix. Each row (along with the user resources) holds the action privileges specific to that user.

(ii) List oriented approach: In this approach, the mechanism associates with each resource a list of users who can access the resource & the action privileges that each user has with respect to the resource. This mechanism operates via a column in the matrix.

70. Explain the various Physical Access Controls relating to an information system.

These are designed to protect the organization from unauthorized access/illegal entry. The authorization given by the management may be explicit, as in a door lock for which management has authorized someone to have a key; or implicit, like a job description which confirms the need to access confidential reports and documents.

Some of the more common access control techniques are –

1. Locks on Door:

Write short notes on 'Locks on Door' with respect to Physical Access Control. Nov 2011

Different types of locks on door for physical security are discussed below:

(i) Cipher Locks: Also known as combination door locks, it consists of push button 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 10 to 30 sec. More sophisticated and expensive cipher locks can be computer coded with a person's handprint. A matching handprint unlocks the door.

(ii) Bolting door locks: A special metal key is used to gain entry when the lock is a bolting door lock.

(iii) Electronic door locks: A magnetic or embedded chip-based plastic 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, activates the door locking mechanism.

Advantages of electronic door lock over bolting and combinational lock are -

♦ Through the special internal code, cards can be made to identify the correct individual.
♦ 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.
♦ An administrative process, which may deal with issuing, accounting for and retrieving the card keys are also parts of security.

(iv) Biometric Door Lock: These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks.

2. Physical Identification Medium:

Write short notes on 'Physical Identification Medium' with respect to Physical Access Control.

(i) Personal identification number(PIN): A secret number will be assigned to the individual, as a means of identifying them and servers to verify the authenticity of the individual. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via PIN keypad. The user's entry will be matched with the PIN number available in the security database.

(ii) Plastic Cards: These cards are used for identification purpose. Controls over cards seek to ensure that customers safeguard their card so it does not fall into Unauthorized hands.

(iii) Cryptographic control: Cryptography deals with transformation of data into codes that are meaningless to anyone who does not possess the system for recovering initial data. Only a crypt analyst can do the transaction.
(iv) Identification Badges: Special identification badges can be issued to personnel as well as visitors. For easy identification purpose their colour of the badge can be changed.

3. Logging on utilities:

Explain the various types of 'Logging on Utilities' with respect to Physical Access Control.

(i) Manual logging: All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Logging may happen at both the front reception and entrance to the computer room.
(ii) Electronic logging: This feature is a combination of electronic and biometric security systems. The users logging in can be monitored and the unsuccessful attempts being highlighted.

4. Other means of controlling Physical Access:

Explain the 'Other Methods/Means of Controlling Physical Access'?

(i) Video Camera: Cameras should be placed at specific location and monitored by security guards. The video supervision recording must be retained for possible play back.
(ii) Security Guards: Extra security can be provided by appointing guard.Guards supplied by an external agency should be made to sign a bond to protect the organizations from loss.
(iii) Controlled visitor Access: A responsible employee should escort all visitors.
(iv) Bonded Personnel: All service contract personnel should be asked to sign a bond.
(v) Dead men doors: These systems consist of a pair of doors that are typically found in entries to facilities such as computer room. The first entry door must close and lock, for the second door to operate, with the only person permitted in the holding area. Only a single person is permitted at a given point of time and this will surely reduce the risk of piggybacking, when an unauthorized person follows an authorized person though secured entry.
(vi) Non-exposure of sensitive facilities: There should be no explicit indication such as presence of directional sign hinting the presence of facilities such as computer rooms.
(vii) Computer terminal locks: These locks ensure that the device to the desk is not turned on or disengaged by unauthorised users.
(viii) Controlled single entry point: A controlled single entry point is monitored by a receptionist. Multiple entry point increase the chances of unauthorized entry.
(ix) Alarm system: Linking alarm system to inactive entry point, motion detector, reverse flows of enter or exit only door can be used to avoid illegal entry.
(x) Perimeter Fencing: Fencing at boundary of the facility may also enhance the security mechanism.
(xi) Control of out of hours of employees: Employees who are out of office for a longer period of time should be monitored carefully.
(xii) Secured Report/Document Distribution cart: These must be covered & locked and should always be attended.

5. Accounting Audit Trail:

Explain how 'Audit Trail' review can be used as a Physical Access Control.

All the activities taken in the system should be properly recorded. The following sorts of data must be kept -
(i) Action privileges requested (ii) Action privileges allowed (iii) Authentication information supplied
(iv) Identity of the perspective user (v) Number of logon attempts (vi) Resources requested
(vii) Resources provided (viii)Start and finish time (ix)Terminal identifier

71. Briefly explain the Audit and Evaluation Techniques for Physical Access.

Information Processing Facility (IPF) is used to gain an overall understanding and perception of the installation being reviewed. Much of the testing of physical safeguard can be visually observation of the safeguard. The documents to assist with this effort include emergency evaluation procedure, inspection, tags, fire suppression system test results and key lock logs.

The facility/computer room should include the following related facilities -
(i) Computer storage rooms (ii) Location of all communication equipment (iii) Location of all operator consoles
(iv) Off-site backup storage facility (v) Printer rooms (vi) Tape library (vii) UPS
To do thorough testing, we have to look above the ceiling panels and below the raised floor in the computer operation center. Keen observation is done on smoke and water detector.

The following paths of physical entry should be evaluated for proper security-
(i) All entrance points (ii) Glass windows and walls (iii) Movable walls and modular cubicles
(iv) Above suspended ceiling & beneath raised floors (v) Ventilation systems

72. Discuss the role of IS auditor with respect to Physical Access Controls. May 2011

Auditing physical access requires the auditor to review the physical access risk and controls. This involves the following -
1) Risk Assessment -The auditor must satisfy that the risk assessment procedure adequately covers periodically and timely assessment of all assets, physical access threats, vulnerabilities of safeguards.
2) Controls Assessment: On the basis of risk profile, the auditor evaluate whether the physical access controls are in place & adequate or not.
3) Review of physical access controls: It requires examination of relevant documentation such as the security policy & procedures.
4) Testing of controls -The auditor should test physical access controls to satisfy that -
(i) Tour of organizational facilities including outsourced and offsite facilities.
(ii) Physical inventory of computing equipment & support infrastructure
(iii) Interviewing personnel
(iv) Observation of safeguard and physical procedure. ***This would also include inspection of*** -
(a) Core computing facilities (b) Computer storage rooms (c) Communication closet (d) Backup and off site facilities
(e) Printer rooms (f) Disposal yards and bins (g) Inventory of supplies and consumables

Some special considerations involved the following -
(a) All points of entry/exit (b) Glass windows and walls (c) Movable and modular cubicles
(d) Ventilation/AC ducts (e) False ceiling and flooring panels
(v) Review of physical access procedures. Employee termination procedure etc.
(vi) Examination of physical access logs and reports.

73. Briefly explain the categories of IS resources from the perspective of Environmental Exposures & Controls.

From the perspective of environmental exposures and controls, information systems resources may be categorized as follows :
i) Hardware and Media: Includes Computing Equipment, Communication equipment, and Storage Media.
ii) IS Supporting infrastructure or Facilities: ***This typically includes the following:***
(a) Physical Premises, like Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities & Storage Areas
(b) Communication Closets (d) Power Source
(c) Cabling ducts (e) Heating, Ventilation and Air Conditioning (HVAC)
iii) Documentation: Physical & geographical documentation of computing facilities with emergency excavation plans & incident planning procedures.
iv) Supplies: The third party maintenance procedures for say air conditioning, fire safety and civil contractors.
v) People: The employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls.

74. Briefly explain the Environment Issues and Exposures.

Environmental exposures are primarily due to elements of nature. However, with proper controls, exposure to these rudiments can be reduced. ***Common occurrences are -***
(i) Fire (ii) Power spike (iii) Electric shock (iv) Equipment failure
(v) AC Failure (vi) Water damage (vii) Natural disasters – earthquake, volcano, hurricane etc. (viii) Bomb attack
***Other environmental issues & revelations include the following*:**
♦ Is the power supply remains within the manufacturer's specification?
♦ Are the AC, humidity and ventilation control systems protected against the effects of electricity rug?
♦ Is consumption of food beverages and tobacco products prohibited?
♦ Are backup media protected from damage due to variations of temperatures?
♦ Is the computer equipment kept free of dust, smoke and other pollutant?

75. Briefly explain the various controls for environmental exposures.

1. Water Detectors: In computer room, water detector should be placed under the raised floor & near drain holes. A remedial action must be instantiated on hearing the alarm by notifying specific individual & allotting the responsibility for investigating the cause.
2. Hand-held fire extinguishers: Fire extinguishers should be placed at the appropriate location throughout the area. They should be tagged for inspection.
3. Manual Fire alarm: Hand-pull alarms should be purposefully placed throughout the facility. The alarm should be linked to a monitored guard station.
4. Smoke Detectors: Smoke detectors are positioned at placed, and upon acceptation these detectors should produce an alarm that must be linked to a monitored station.
5. Fire Suppression system: These alarms are activated when extensive heat is generated de to fire. The system should be segmented so that fire in one part of a large facility does not activate the entire system. The fire suppression techniques are –
a) Dry-pipe sprinkler systems: The advantage of such systems is that any failure in the pipe will not result in water leaking into the sensitive equipment.
b)Water based system: These systems are effective but not popular because they damage equipment & property.
c) Halon gas system: They contain pressurized halon gases that remove oxygen from the air. It is preferred to others because it does not damage equipment like water does. Its disadvantage is that it adversely affects the ozone layer.
6. Strategically locating the computer room: To reduce the risk of flooding, computer room should not be located in the basement of a multi-storied building.
7. Regular inspection by fire department: To ensure that all fire detection systems act in accordance with building codes.
8. Fireproof walls, floor and ceilings: The surrounding walls should have at least one or two hour fire resistance rating.
9. Electrical surge protectors: They reduce the risk of damage due to power spikes & are typically built into the UPS.
10. Un-interruptible Power Supply / Generator: In case of power failure, the UPS provides the back up by providing electrical power from the generator to the computer for a certain span of time.
11. Power leads from two Substations: In this way, the interruption of one power supply does not affect electrical supply.
12. Emergency Power-off switch: Two emergency power off switch one at computer room and other near but outside the computer room would serve the purpose. They should be easily accessible and yet secured from unauthorized people.
13. Wiring placed in electrical panels and conduit: It helps to reduce the risk of electrical fire.
14. Prohibition against eating, drinking & smoking within the Info Processing Facility(IPF): This prohibition should be clear.
15. Fire resistant office furniture: i.e material used in IPF such as desks, cabinets etc should be fire resistant.

76. Briefly explain the Audit and Evaluation Techniques for environmental controls.

1. Water and Smoke detectors: The presence of water and smoke detector are verified on visiting the computer room. Also checks adequacy of power supply to these detectors.
2. Hand-held Fire Extinguishers: The presence of fire extinguishers in strategic locations throughout the facility is checked for.
3. Fire suppressions systems: Testing of suppressions systems becomes more expensive, hence reviewing documentation that has been inspected and tested within the last year ensures it.

4. Regular inspection by fire department: The person responsible for fire equipment maintenance is contacted and also the employees are queried, whether, fire department inspector has been invited.
5. Fire proof walls, floors and ceilings Surrounding the computer room: Identifies the fire rating of the walls surrounding the information processing facility are done. These walls should have at least a two-hour fire resistance rating.
6. Electrical surge protector: The presence of electrical surge protector for sensitive and expensive computer equipment is observed.
7. Power leads from two substation: Checking the use & replacement of redundant power lines into the info processing facility.
8. Fully Documented and tested business continuity plan: (Covered in Chapter 8)
9. Wiring placed in electrical panels and conduit: Checking of whether the wiring in the information processing facility is placed in the fire-resistant panels and conduit is done.
10. Documented and tested emergency evacuation plans: A direct interview of the employees is conducted to test whether the emergency plans are posted throughout the facilities.
11. Humidity/Temperature control: To visit on regular intervals and physically determine if temperature and humidity are adequate.

77. Discuss the role of IS auditor with respect to Environmental Controls. ***Practice Manual***

Audit of environmental controls should form a critical part of every IS audit plan. The IS auditor should satisfy that the overall controls assure safeguard the business against environmental risks.

***The critical factors that auditor should take into account while conducting his audit are*:**

1. Audit Planning and Assessment: As part of risk assessment -

♦ The risk profile should include the different kinds of environmental risks that the organization is exposed to.
♦ The control assessment must ascertain that controls safeguard the organization against all acceptable risks are in place.
♦ Security policy of the org'n should be reviewed to assess policies & procedures that safeguard the org'n against environmental risks.
♦ Building plan and wiring plans need to be reviewed to determine the appropriateness of location of IPF.
♦ The IS auditor should relevant interview personnel to satisfy about employees' awareness of environment threats and controls.
♦ Administrative procedures such as preventive maintenance plans,incidents reporting and handling procedures need to be reviewed.

2. Audit of Technical Controls: Audit of environmental controls requires the IS auditor to conduct physically inspection and observe practices. He must verify:

♦ The IPF and the construction with regard to the type of material used for construction.
♦ The location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers.
♦ The presence of water & smoke detector, power supply arrangements.
♦ Emergency procedures, evacuation plans and marking of fire exits. If necessary, the IS auditor may also use a mock drill.
♦ Documents for compliance with legal and regulatory requirement with regard to fire safety equipment, external inspection
♦ Environmental controls requirement such as air-conditioning, dehumidifiers, heaters, ionizers etc.
♦ Compliant logs and maintenance logs to assess whether MTBF and MTTR are within acceptable levels.
♦ Activities in the IPF. Identify undesired activities such as smoking, consumption of eatable etc.

Documentation: As part of the audit procedure, the IS auditors should also document all findings. The working paper could include audit assessments, audit plans, audit procedures, questionnaires, interview sheets, inspection charts etc.

Chapter 4 : Testing - General and Automated Controls

1. What do you mean by Testing and what are the Reasons for testing of controls? Nov 2008
Explain the term Testing w.r.t Controls. Also define Substantive & Compliance Testing. RTP May 2012

Testing: It is a scientific process performed to determine whether the controls ensure -
- ✓ Effectiveness of system design, and
- ✓ Operational effectiveness of implemented system controls.

It involves an understanding of process and the expected results.

Testing of Controls: It involves obtaining the population & conducting the compliance tests either on the entire population or/and on selected samples from the population.It may also be conducted using utilities of audit tools.

Briefly explain the methods for testing the control design and reliable results.

Testing of controls design & the reliable results are done by one of the following methods:

(i) Substantive Testing: This type of testing is used to substantiate the integrity of the actual processing and to ensure that the processes are working as per the design of the control & produce the reliable results.

(ii) Compliance Testing: This testing is used to determine whether the controls are working as designed & adhere to mgt directives.

2. Briefly explain the three phases of Info system (IS) controls audit.

Phase - I - Audit Planning:

(1) In planning the IS controls audit, the auditor uses the equivalent **concepts of materiality** ***(in Financial Audits)*** **and significance** ***(in Performance Audits)*** to plan both effective & efficient audit procedures.These concepts are used to determine the planned nature, timing, and extent of audit procedures.**The underlying principle** is that the auditor is not required to spend resources on the items of little importance; i.e those that would not affect the judgment or conduct of a reasonable user of the audit report.

(2) **Materiality & significance** include both quantitative & qualitative factors in relation to the subject matter of audit. Even though a system may process transactions that are quantitatively immaterial or insignificant, the system may contain sensitive info or provide an access path to other systems that contain info which is sensitive or material/significant.

(3) Though planning activities are concentrated in planning phase, it occurs throughout the audit as an iterative process.

Phase - II - Audit Testing {Practice Manual}:

The auditor must address many considerations that cover the nature, timing, and extent of testing. For this purpose, he does the audit testing in following manner:
- ➢ He must devise an audit testing plan & a testing methodology to test the effectiveness of previously identified controls.
- ➢ He also tests whether the end-user applications are producing valid & accurate info.
- ➢ Depending on the nature of the audit, the auditor may also use the computer-assisted techniques to audit the application.
- ➢ The auditor should also conduct several tests with both valid & invalid data to test the ability & extent of error detection, correction, & prevention within the application.
- ➢ The auditor performs the necessary testing by using documentary evidence, corroborating interviews, & personal observation. It calls for validation in several ways as follows:

a) Asking different personnel the same question & comparing the answers.
b) Asking the same questions in different ways at different times.
c) Comparing checklist answers to work papers, programs, documentation, tests, or other verifiable results.
d) Comparing checklist answers to observations & actual system results.
e) Conducting mini-studies of critical phases of the operation.

Such an intensive program allows an auditor to become informed about the operation in lesser time. The audit team selects one of the Generalized Audit Software (GAS) packages **such as** Microsoft Access or Excel, IDEA, or ACL and determines what changes are necessary to run the software at the installation.

Phase - III - Audit Reporting:

After completing the testing phase, the auditor summarizes the results of audit, draws conclusions on the individual & aggregate effect of identified IS control weaknesses on audit risk & audit objectives and reports the results of audit. The auditor evaluates the following:

(i) Individual & aggregate effect of all identified IS control weaknesses on the auditor's conclusions & the audit objectives.

(ii) The effect of any weaknesses on the entity's ability to achieve each of the critical elements & on the risk of unauthorized access to key systems or files.

(iii) The potential control dependencies.

(iv) The effect of related underlying control activities that are not achieved.

(v) Whether the aggregate combination of weaknesses could result in unauthorized access to systems or files supporting key areas of audit interest.

(vi) The potential impact of any identified weaknesses on the completeness, accuracy, validity, and confidentiality of application data relevant to the audit objectives.

The auditor should make a summary determination as to the effectiveness of the entity's related controls, considering entity-wide, system, and business process application levels collectively.

3. Explain the process of IS Controls Audit. How does an auditor obtain necessary info related to this?

The process of IS controls audit involves:

(i) Obtaining an understanding of an entity & its operations and key business processes;

(ii) Obtaining a preliminary understanding of IS controls;

(iii) Obtaining a general understanding of the structure of the entity's networks;

(iv) Identifying key areas of audit interest; and

(v) Identifying critical control points.

These tasks are not generally performed as discrete, sequential steps, The auditor performs planning to determine an effective &

efficient way to obtain the evidential matter necessary to support the objectives of IS controls audit & the audit report. The nature & extent of audit planning procedures varies for each audit depending on several factors, including the entity's size & complexity, the auditor's experience with the entity, and the auditor's knowledge of the entity's operations. The auditor may obtain the necessary info in the following manner:

- ✓ Through interviews with key IT staff; or
- ✓ Through data requests.

4. What are the Auditor's duties when IS Controls Audit is performed as a part of Financial Audit?

If the IS controls audit is performed as a part of Financial audit, the auditor is to obtain an understanding of internal control over financial reporting sufficient to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing, and extent of further audit procedures based on that assessment. This includes performing risk assessment procedures to evaluate the design of controls relevant to an audit of financial statements and to determine whether they have been implemented. In obtaining this understanding, the auditor considers how an entity's use of IT & manual procedures affect controls relevant to the audit.

5. What are the Auditor's duties when IS Controls Audit is performed as a part of Performance Audit?

If the IS controls audit is performed as a part of Performance audit, the auditor should then evaluate the design & operating effectiveness of such controls. This evaluation would include other IS controls that impact the effectiveness of the significant controls or the reliability of info used in performing the significant controls. Auditors should obtain a sufficient understanding of IS controls necessary to assess audit risk & plan the audit within the context of the audit objectives.

6. What are the factors that assist the auditor in determining the audit procedure relating to IS Controls?

Auditors need to determine which audit procedures related to IS Controls are needed to obtain sufficient, appropriate evidence to support the audit findings & conclusions. It also provides some factors to assist the auditor in making this determination. Explain those factors, in brief. Practice Manual

These factors are given as follows:

(i) **Extent to which internal controls are significant to the audit:** It depends on the reliability of info processed or generated by IS.

(ii) **Availability of evidence outside IS to support the findings & conclusions:** It may not be possible for auditors to obtain sufficient, appropriate evidence without assessing the effectiveness of relevant IS controls.

(iii) **Relationship of IS controls to data reliability:** To obtain the evidence about reliability of computer generated info, auditors may decide to assess the effectiveness of IS controls as part of obtaining evidence about the reliability of data. If the auditor concludes that IS controls are effective, the auditor may reduce the extent of direct testing of data.

(iv) **Assessing the effectiveness of IS controls as an audit objective:** When assessing the effectiveness of IS controls is directly a part of audit objective, the auditors should test IS controls necessary to address the audit objectives.

7. How should an Auditor identify the key areas of Audit Interest?

The auditor should identify the key areas of audit interest, which are those that are critical to achieving the audit objectives.

Example - (i) for a financial audit, this would include the key financial applications & data and related feeder systems.

(ii) For a performance audit, this would include key systems that are likely to be significant to the audit objectives. For each key area of audit interest, the auditor should document relevant general support systems & major applications & files, including

- ✓ The operational locations of each key system or file,
- ✓ Significant components of the associated hardware & software,
- ✓ Other significant systems or system level resources that support the key areas of audit interest, and
- ✓ Prior audit problems reported.

The auditor should also identify all access paths into & out of the key areas of audit interest. By identifying the key systems, files, or locations, the auditor can concentrate efforts on them & do little or no work associated with other areas. The auditor generally should prioritize important systems, files, or locations in order of importance to the audit objectives.

8. List the info to be documented by the Auditor in the preliminary understanding of design of IS controls.

Explain the info which should be included by auditors in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives. Practice Manual

The auditor should include the following info in the documentation of their preliminary understanding of the design of IS controls, to the extent relevant to the audit objectives:

1. Identification of entity-wide level controls;
2. Identification of business process level controls;
3. Any internal or third party IS reviews, audits, or specialized system testing;
4. Status of prior years' audit findings;
5. Current multi-year testing plans;
6. Documented security plans;
7. Documented risk assessments for relevant systems;
8. Documented BCPs and DRPs;
9. A description of entity's use of third party IT services;
10. Relevant laws & regulations and their relation to the audit objectives.

9. Explain the Three-Level test for performing IS Control Audit.

The auditor identifies control techniques & determines the effectiveness of controls at 3 levels. Explain in brief those levels.

These levels are:

1. Entity wide or Component level (General controls): Controls at entity or component level consist of entity-wide or component -wide processes that are designed to achieve the control activities. The absence of entity-wide processes may be a root cause of weak or inconsistent controls i.e. IS controls are not consistently applied across the organization.

2. System level (General controls): These controls are more specific than those at the entity or component level & generally relate to a single type of technology. There are three sub-levels that the auditor should assess:
(i) **Network controls:** A network is an inter-connected or intersecting configuration or system of components. **For example -** A computer network allows applications operating on various computers to communicate.
(ii) **Operating system:** An operating system is a software that controls the execution of computer programs & may provide various services. **For example -** An operating system may provide services such as resource allocation, scheduling, input/output control, and data mgt.
(iii) **Infrastructure applications:** These are the software that are used to assist in performing system operations and include databases, e-mail, browsers, plug-ins, utilities, and applications not directly related to business processes.
3. Business process application level: Controls at this level consist of policies & procedures for controlling specific business processes. **For example -** The entity's configuration mgt should reasonably ensure that all changes to application systems are fully tested & authorized.
The control techniques for achieving the control activities & the related audit tests vary according to the level to which they are being applied. Thus, the auditor should develop more detailed audit steps based on the entity's specific software & control techniques, after consulting with the financial or performance auditor about audit objectives & significant areas of audit interest.

10. What are the Auditor's duties i.r.t "Testing of Critical Control Points"?

1. The auditor should evaluate the effectiveness of IS controls including the system auditor application level controls related to each control point.
2. The auditor should evaluate all potential ways in which the critical control points could be accessed. This would include assessing controls related to network, operating system, and infrastructure application components.
For example - If a particular router was deemed to be a critical control point, then, the auditor should test controls related to the router itself, its operating system, and the infrastructure application which is used to manage the router.
3. The auditor determines the appropriate scope of IS control audit, including the organizational entities to be addressed; the breadth of the audit; the types of IS controls to be tested etc.

11. How does an Auditor test the effectiveness of IS Controls?
Explain the test effectiveness of IS Controls. **Practice Manual**

It is generally more efficient for the auditor to test IS controls on a tiered basis, starting with the general controls at the entity wide & system levels, followed by the general controls at the business process application level. If the auditor identifies IS controls for testing, the auditor should evaluate the effectiveness of:

- General controls at the entity wide & system level;
- General controls at business process application level; and
- Specific business process application controls, and/or user controls, unless the IS controls that achieve the control objectives are general controls.

The auditor should determine whether entity wide & system level general controls are effectively designed, implemented, and operating effectively by:

- Identifying applicable general controls;
- Determining how those controls function, and whether they have been placed in operation; and
- Evaluating & testing the effectiveness of the identified controls.

The auditor should document the understanding of general controls & should conclude whether such controls are effectively designed, placed in operation and operating as intended.

12. How does an auditor test general controls at entity-wide and system levels?

1. In order to test the general controls, the auditor uses a combination of procedures including observation, inquiry, inspection, & re-performance using appropriate test software. He may also use sampling to test certain controls, such as those involving approvals.
2. ***If general controls*** at entity wide & system levels ***are not effectively designed and operating*** as intended, the auditor will generally be unable to obtain satisfaction that business process application-level controls are effective. In such instances, the auditor should:

- Determine & document the nature & extent of risks resulting from ineffective general controls and
- Identify & test any manual controls that achieve the control objectives, that the IS controls were to achieve.

3. However, if the manual controls do not achieve the control objectives, the auditor should determine whether any specific IS controls are designed to achieve the objectives. If not, the auditor should develop appropriate findings to provide recommendations to improve internal control.

13. How does an auditor test general controls at Business Process Application Level?

1. If the auditor reaches a favorable conclusion on general controls at the entity wide & system levels, the auditor should evaluate & test the effectiveness of general controls for those applications within which business process application controls or user controls are to be tested. These business process application level general controls are referred to as **Application Security (AS) controls.**
2. If the general controls are not operating effectively within the business process application, then, the business process application controls & user controls will be ineffective. The auditor should determine whether to proceed with the evaluation of business process application controls & user controls.

14. How does an auditor test Business Process Application Controls and User Controls?

The auditor should determine the controls necessary to achieve the control objectives where the entity-wide system & application level general controls were determined to be effective. If IS controls are not likely to be effective, the auditor should obtain a sufficient understanding of control risks arising from info systems to:

- Identify the impact on the audit objectives,
- Design audit procedures, and
- Develop appropriate findings.

The auditor also determines whether manual controls achieve the control objectives. If IS controls are not likely to be effective & if manual controls do not achieve the control objectives, the auditor should identify & evaluate any specific IS controls that are designed to achieve the control objectives.
If the auditor determined in a prior year that controls in a particular accounting application were ineffective and if mgt indicates that controls have not significantly improved, then, the auditor need not test them.

15. How will an Auditor test the appropriateness of control tests?

To assess the operating effectiveness of IS controls, auditors should perform an appropriate mix of audit procedures to obtain sufficient, appropriate evidence to support their conclusions. Explain these procedures, in brief. Practice Manual

Such procedures could include the following:

1. Inquiries of IT & Mgt personnel: It can enable the auditor to gather a wide variety of info about the operating effectiveness of control techniques.

2. Questionnaires: These can be used to obtain info on controls & how they are designed.

3. Observation of the operation of controls: It provides evidence about controls only when the auditor was present.

4. Reviewing documentation of control policies & procedures: It will allow the auditors to understand & assess the design of controls.

5. Inspection of approvals/reviews: It provides the auditor with evidence that mgt is performing appropriate control checks.

6. Analysis of system info: It provides the auditor with evidence about actual system configuration.

7. Use of CAAT to test data files: It may be used to determine whether invalid transactions were identified & corrected by the programmed controls.

8. Re-performance of control: It could be used to test the effectiveness of some programmed controls by re-applying the controls through the use of test data.

9. **Determining the operating effectiveness of control techniques to achieve the control activities:** Based on the results of IS controls audit tests, the auditor determines that the controls that are not properly designed to achieve the control activities or controls that are not operating effectively are potential IS control weaknesses.

10. Determining the specific compensating controls: For each potential weakness, the auditor should determine whether there are specific compensating controls or other factors that could mitigate the potential weakness.

16. Write short notes on "Multiyear Testing Plans".

1. Where the auditor regularly performs IS controls audits of the entity, he may determine that a multi year plan for performing IS controls audit is appropriate.
2. Such a plan will cover relevant key agency applications, systems, and processing centres.
3. These strategic plans should cover **not more than a three year period.** The auditor typically evaluates these plans annually & adjusts them for the results of prior & current audits and significant changes in IT environment.
4. Under a multi year testing plan, different controls are comprehensively tested each year, so that each significant general & business process control is selected for testing at least once during the multi year period.
5. However, such multi year testing plans are not appropriate in all situations. **For Example -** These plans are not appropriate for:

- ❖ first-time audits;
- ❖ for audits where some significant business applications or general controls have not been tested within a sufficiently recent period; or
- ❖ for audits of entities that do not have strong entity wide controls.

17. List the info to be documented by the Auditor in the Testing Phase of IS Controls.

Explain the info developed in the testing phase that the auditor should document. Practice Manual

Info developed in the testing phase that the auditor should document includes the following:

(i) An understanding of the IS that are relevant to the audit objectives;

(ii) IS control objectives & activities that are relevant to the audit objectives;

(iii) By level & system sub-level, a description of control techniques used by the entity to achieve the relevant IS control objectives & activities;

(iv) By level & sub-level, specific tests performed including related documentation that describes the nature, timing, & extent of tests;

(v) If a control is not achieved, any compensating controls or other factors & the basis for determining whether they are effective;

(vi) The auditor's conclusions about the effectiveness of the entity's IS controls in achieving the control objective; and

(vii) For each weakness, whether the weakness is a material weakness, significant deficiency or just a deficiency, as well as the criteria, condition, cause, & effect if necessary, to achieve the audit objectives.

18. Bring out the need for Continuous/Concurrent Audit Techniques. Nov 2004

There is a need for continuous/concurrent audit techniques due to the following reasons:

1. Real-time recordings: Today, organizations produce info on a real-time, online basis. Real-time recordings need real-time auditing to provide continuous assurance about the quality of data, thus, continuous auditing.

2. Time reduction b/w occurrence of events & auditor's assurance services: Continuous auditing enables auditors to significantly reduce the time b/w occurrence of client's events & the auditor's assurance services thereon.

3. For early detection of errors: Errors in a computerized system are generated at high speeds & at the cost to correct and return programs are high. If these errors can be detected & corrected at the point or closest to the point of their occurrence, the impact thereof would be the least.

19. Briefly explain the different types of Audit Tools/Techniques.

1. Snapshots: (May 2007) This technique can be used to trace the transactions in a computerized system. The snapshot software is built into the system at those points where material processing occurs which takes images of flow of any transaction as it

moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. **The main areas to be considered while using snapshots are:**
(i) To locate the snapshot points based on materiality of transactions;
(ii) When the snapshot will be captured; and
(iii) The reporting system design & implementation to present data in a meaningful way.
2. **Integrated Test Facility (ITF): {Nov 2006}** This technique involves the **creation of a dummy entity** in the application system files & the processing of audit test data against the entity, as **a means of verifying** processing authenticity, accuracy, & completeness. This 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 & the methodology for removal of effects of the ITF transactions.
Methods of Entering Test Data:
(i) Tagging of transactions: The transactions to be tested have to be tagged. The application system has to be programmed to recognize the tagged transactions & have them invoke two updates i.e. one to the application system master file record and other 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.
(ii) Use of special test data: The auditors may also use test data which 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 & the application system does not have to be modified to tag the ITF transactions & to treat them in a special way. However, preparation of test data could be time consuming & 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 in any of the following manner:
(i) The application system may be programmed to recognize ITF transactions & to ignore them in terms of any processing that might affect users.
(ii) Additional inputs may be submitted that may reverse the effects of ITF transactions.
(iii) Another less used approach is to submit **Trivial Entries** so that the effects of ITF transactions on the output are minimal.
3. System Control Audit Review File (SCARF): Practice Manual
Meaning of SCARF: In many ways, this technique is similar to snapshot technique along with other data collection capabilities. The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The info collected is written onto a special audit file called the SCARF master files. Auditors then examine the info contained on this file to see if some aspect of the application system needs follow-up.
Which types of info may be collected by the auditors by using SCARF? **Practice Manual; May 2011; RTP Nov 2012**
"As an IS Auditor, explain the types of info collected for auditing by using SCARF technique." **May 2013**
Auditors might use SCARF to collect the following types of info:
(i) Snapshots & extended records: Snapshots & extended records can be written into the SCARF file & printed when required.
(ii) Application system errors: SCARF audit routines provide an independent check on the quality of system processing i.e. whether there are any design & programming errors as well as errors that could creep into the system when it is modified & maintained.
(iii) Policy & procedural variances: Organizations have to adhere to the policies, procedures & 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 & standards have occurred.
(iv) System exception: SCARF can be used to monitor different types of application system exceptions.
(v) Statistical sample: SCARF provides a convenient way of collecting all the sample info together on one file & use analytical review tools thereon.
(vi) Profiling data: Auditors can use embedded audit routines to collect data to build profiles of system users.
(vii) Performance measurement: Auditors can use embedded routines to collect data which is useful for measuring or improving the performance of an application system.
4. Continuous & Intermittent Simulation (CIS): Practice Manual
This is a variation of SCARF audit technique. This technique can be used to trap exceptions whenever the application system uses a DBMS. During application system processing, CIS executes in the following way:
- The DBMS 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 DBMS.
- 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 b/w the results it produces & those the application system produces.
- Exceptions identified by CIS are written to exception log file.

Advantage of CIS: It does not require modifications to the application system & yet provides an online auditing capability.
20. Explain the Advantages & Disadvantages of using Continuous Audit Techniques. Practice Manual; Nov 2011
Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system & operations" audit.
Advantages of Continuous Audit Techniques: May 2010; RTP Nov 2012; RTP Nov 2013
1. Timely, comprehensive & detailed auditing: Evidence would be available more timely & in a comprehensive manner. The entire processing can be evaluated & analyzed rather than examining the inputs & the outputs only.
2. Surprise test capability: As the evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the system staff & application system users being aware that the evidence is being collected at that particular moment.

3. Info to system staff on meeting of objectives: Continuous audit techniques provide info to system 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.

4. Training for new users: Using the ITFs new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

Disadvantages of Continuous Audit Techniques: **RTP May 2012, RTP May 2014**

1. Availability of resources: Auditors should be able to obtain the resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.

2. Auditor's involvement in system development: Such techniques are more likely to be used if auditors are involved in the development work associated with a new application system.

3. Auditors knowledge on the working of systems: Auditors need the knowledge & experience of working with the computer systems, to be able to use these techniques effectively & efficiently.

4. Missing Audit Trail: Such techniques are more likely to be used where the audit trail is less visible and the cost of errors & irregularities are high.

5. Stable Application System: These techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

21. Why is there need for "Hardware Testing" and what are its types?

Hardware testing may be done to the entire system against the Functional Requirement Specifications (FRS) and/or the System Requirement Specification (SRS). Focus is to have almost a destructive attitude and test not only the design, but also the behavior & even the believed expectations.

Types of Hardware Testing -

(i) Functional testing (ii) User interface testing (iii) Usability testing (iv) Compatibility testing
(v) Model based testing (vi) Error exit testing (vii) User help testing (viii) Security testing
(ix) Capacity testing (x) Performance testing (xi) Reliability testing (xii) Recovery testing
(xiii) Installation testing (xiv) Maintenance testing (xv) Accessibility testing

22. What are the areas that an Auditor has to review in case of Hardware?

1. Review of Capacity Mgt Procedures for hardware & performance evaluation procedure: To determine:

- Whether such procedures ensure continuous review of performance & capacity in terms of hardware, software, networks, user needs, business needs, mgt objectives & service levels.
- Whether historical data & analysis obtained from the IS trouble logs, processing schedules, job accounting system reports, preventive maintenance schedules & reports are used in IS mgt's hardware performance monitoring
- Ensure that the technical mgt's decision to acquire or dispose off computing related hardware & software are indeed based on results of capacity planning models & workload forecasts tempered with good business judgment.

2. Review of Hardware Acquisition Plan:

During the review of hardware, how will you review the hardware acquisition plan? **RTP May 2013, RTP May 2014**

The auditor should review this area to determine:

- Whether the hardware acquisition plan is in concurrence with the strategic business plan of mgt.
- Whether the IS mgt has issued written policy statements regarding the acquisition of hardware.
- Whether the criteria for the acquisition of hardware are laid out to facilitate the acquisition approval process.
- Whether there is awareness of budget constraints.
- Whether the requests for the acquisition of hardware are supported by cost/benefit analysis.

3. Review of Change in Mgt Controls:

During the review of hardware, how will you review the change in mgt controls? **Nov 2012**

During the review of hardware, review in the change mgt control is accomplished by the following:

(i) Ensure that there is a cross-reference b/w the change & its cause.
(ii) Determine whether the changes to H/W configuration are planned & timely info is given to the individual responsible for scheduling.
(iii) Ascertain whether the system programmers, application programmers & the IS staff have been informed of all H/W changes.
(iv) Determine whether the change schedules allow time for adequate installation & testing of new hardware.
(v) Verify that the operator documentation is properly updated to reflect changes in hardware.

4. Review of Preventive Maintenance Practices:

During the review of hardware, what are the tasks, which should be accomplished by a reviewer to evaluate the adequacy & the timeliness of preventive maintenance? **RTP Nov 2013**

During the review of hardware, **major tasks, which should be accomplished** by a reviewer to evaluate the adequacy & the timeliness of preventive maintenance, **are given as follows:**

- To understand the frequency of scheduled preventive maintenance work performed by the hardware vendors;
- To compare this frequency to hardware maintenance contract & note any exceptions;
- To determine compliance with maintenance contractual agreements by examining maintenance log;
- To ascertain whether scheduled maintenance has had any adverse effect on the production schedule during peak season;
- To determine whether preventive maintenance logs are retained.

23. Explain the approach to be adopted by an IS Auditor while testing Operating Software, Acquisition or Maintenance.

While testing the operational software development, acquisition or maintenance, the following approach may be adopted:

1. Interview the technical service manager, system programming manager, & other personnel regarding implementation procedures, documentation requirements etc.
2. Review the feasibility study & selection process to determine the proposed system objectives.

3. Review the cost/benefit analysis of system software procedures to determine they have addressed the direct financial costs associated with the product, cost of product maintenance, and impact on data security etc.
4. Review controls over the installation of changed system software to determine that all appropriate levels of the software have been implemented & that predecessor updates have taken place.
5. Review system software maintenance activities to determine that the changes made to the system software are documented.
6. Review systems documentation specifically in the areas of installation control statements, parameter tables, & exit definitions.
7. Review & test systems software implementation to determine adequacy of controls in change procedures, authorization procedures, & audit trails etc.
8. Review authorization documentation procedure to determine whether additions, deletions or changes to access authorization have been documented.
9. Review system software security.
10. Review database supported info system controls to determine that the access to shared data is appropriate & the data organization is appropriate.

24. The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. So, what info a reviewer/IS Auditor should identify & understand prior to commencing a LAN review? May 2012

The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. **The reviewer should identify the following:**

1. LAN administrator
2. LAN uses, including main applications used over the network
3. Significant groups of LAN users
4. Significant LAN components
5. LAN topology & network design
6. Network topology

In addition, **the reviewer should gain an understanding of the following:**

- ✓ Functions performed by the LAN administrator
- ✓ LAN transmission media & techniques, including bridges, routers & gateways.

Understanding the above info should enable the viewer to make an assessment of the significant threats to the LAN, together with the potential impact & probability of occurrence of each threat. Having assessed the risks to the LAN, the reviewer should evaluate the controls used to minimize the risks.

25. What are the areas to be reviewed by an IS Auditor to test the "Physical Security" in a LAN Environment? While reviewing a network, what are the tasks, which should be accomplished by a reviewer to test the physical security? RTP May 2013

To test the physical security, a reviewer should perform the following:
(i) Inspect the LAN wiring closet & transmission wiring and verify that they are physically secured.
(ii) Observe the LAN file server computer & verify that it is secured in a manner to reduce the risk of removal of components & the computer itself.
(iii) Obtain a copy of key logs for the file server room & the wiring closet; match the key logs to the actual keys that have been issued and determine that all keys held are assigned to the appropriate people.
(iv) See whether LAN operating manuals & documentation are properly secured.

26. What are the areas to be reviewed by an IS Auditor to test the "Environmental Security" in a LAN Environment?

To test the environmental controls, a reviewer should visit the LAN file server facility & verify that:
(i) Temperature & humidity are adequate.
(ii) Static electricity guards are in place.
(iii) Electric surge protectors are in place.
(iv) Fire extinguishers are nearby.
(v) LAN logical security controls should be in place to restrict, identify & report authorized & unauthorized users of LAN.
(vi) A LAN workstation should be disabled automatically after a short period of inactivity.
(vii) Remote access to the system supervisor should be prohibited and all logon attempts to the supervisor a/c should be logged on in the computer system.
(viii) The LAN supervisor should maintain up-to-date info about all communication lines connected to outside.

27. What are the areas to be reviewed by an IS Auditor to test the "Logical Security" in a LAN Environment?

To test logical security, a reviewer/auditor should interview the person responsible for maintaining LAN security to ensure that the person is:

- ✓ Aware of the risks associated with physical & logical access that must be minimized.
- ✓ Aware of the need to actively monitor logons & to account for employee changes.
- ✓ Knowledgeable in how to maintain & monitor access.

28. How does an IS Auditor review the users' awareness of mgt policies regarding LAN security & confidentiality?

The reviewer/Auditor should perform the following interview users to access their awareness of mgt policies regarding LAN security & confidentiality:
(i) He reviews a sample of LAN access change requests & determine whether it is authorized by the appropriate mgt.
(ii) He reviews a sample of security reports to:
(a) Ensure that only authorized access is occurring;
(b) Verify that timely & effective review of these reports is occurring & that there is an evidence of the review.
(iii) He evaluates a sample of LAN users' access/security profiles to ensure that the access is appropriate & authorized based on the individual's responsibilities.
(iv) He looks for un-authorized users. If found, then he determines the adequacy & timeliness of follow-up procedures.
(v) He attempts to gain access by using a variety of un-authorized logon-IDs/passwords to verify that access is denied & logged.

Chapter 5 - Risk Assessment Methodologies and Applications

1. Explain the following terms in the context of Risk: Nov 2008, RTP May 2012
(i) Asset (ii) Vulnerability (iii) Threat (iv) Exposure (v) Likelihood (vi) Attack (vii) Risk (viii) Countermeasure

(i) Asset: It can be defined as something of value to the organization **E.g.** Info in electronic form, s/w systems, employees etc.

Characteristics of Assets:

- ❖ They are recognized to be value to the organization.
- ❖ They are not replaceable without cost, skill, time, resources or a combination.
- ❖ They form a part of the organization's corporate identity, without which, the organization may be threatened.
- ❖ Their data classification would normally be **Proprietary, Highly Confidential, or even Top Secret.**

It is the duty of the info security personnel to identify the threats against the risks & the associated potential damage to, & the safeguarding of info assets.

(ii) Vulnerability: It is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in info system, cryptographic system (security system), or other components that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.

E.g. Leaving the front door unlocked; short passwords.

(iii) Threat: Any entity, circumstance, oe 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. It has capability to attack on a system with intent to harm.

(iv) Exposure: An exposure is the extent of loss, the organization has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run.

E.g. Loss of business, failure to perform the system's mission and loss of reputation.

(v) Likelihood: It is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, strengths of threats and effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

(vi) Attack: It is an attempt to gain unauthorized access to the system's services to compromise the system's dependability & CIA (i.e confidentiality, integrity & availability), or any other desired feature of an info system. It is an act of trying to defeat IS safeguards. The type of attack & its degree of success determines the consequence of the attack.

(vii) Risk: It is the likelihood that an organization would face a vulnerability being exploited or a threat becoming harmful. Info systems can generate many direct & indirect risks. These risks lead to a **gap b/w** the need to protect systems & the degree of protection applied. Some of the factors that cause gaps are:

- ✓ Widespread use of technology;
- ✓ Inter-connectivity of systems and
- ✓ Devolution of mgt & control etc.

(viii) Countermeasure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is called countermeasure. **E.g.** The well known threat 'Spoofing the user identity' has two countermeasures:

- ✓ Strong authentication protocols to validate users; and
- ✓ Passwords should not be stored in configuration files, instead some security mechanism should be used.

2. What are the general threats in a computer environment? Nov 2008, May 2010, RTP May 2014
"There are always some common threats in a computerized environment". Explain these threats. May 2011

Computerized environment depends on people as they are critical links in making the entire enterprise computing happen. Thus, people are the main source of threat. Threats also arise on a/c of external dependence. A few common threats to computerized environment are as follows:

1. **Power failure:** It can cause disruption of entire computing equipments since computing equipments depend on power supply.
2. **Communication failure:** It results in inability to transfer data, which primarily travel over communication lines. Where the organization depends on public communication lines, the communication failure present a significant threat that will have a direct impact on operations.
3. **Downtime due to technology failure:** Info system facilities may become unavailable due to technical problems or equipment failure & hence, the computing infrastructure may not be available for short or extended periods of time.
4. **Disgruntled employees:** Such employees present a threat as they are having access to sensitive info of the organization. They may cause intentional harm to the info processing facilities.
5. **Abuse of access privileges by employees:** On the basis of job responsibilities of employees, the security policy of the company authorizes them to access & execute selected functions in critical applications.
6. **Errors & Omissions:** These threats are usually occurred in computing environment that threat to data & system integrity. These errors are caused by data entry clerks & by users who create & edit data. To reduce the no. & severity of errors & omissions, a sound awareness & training program should be organized.
7. **Malicious code:** It refers to viruses, worms, trojan horses, logic bombs, & other such software, which freely accesses the unprotected networks and may affect the organizational & business networks that use these networks.
8. **Theft or destruction of computing resources:** Any threat or destruction of the resource can result in compromising the competitive advantage of the organization.
9. **Natural disasters:** These may be earthquakes, lightening, floods, tornado, tsunami, etc. that can adversely affect the functioning of IS operations.
10. **Fire etc.:** Fire due to electric short circuit or due to riots, war or such other reasons, can cause a great damage to the IS infrastructure.

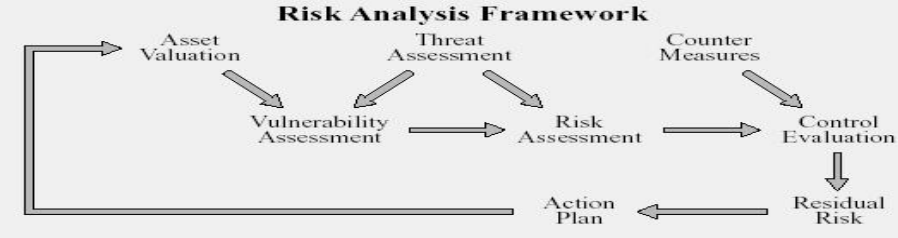
3.List the threats in a computer environment due to Cyber Crimes. June 09, Nov 09, Nov 12, RTP Nov 12 & 13

Following are the major threats due to cyber crimes:

1. Embezzlement: It is unlawful misappropriation of money or other things of value, by the persons to whom it was entrusted (usually employees), for their own use or purpose.
2. Fraud: It occurs on a/c of intentional misrepresentation of info or identity to deceive others. It may be committed by someone inside or outside the company. **E.g.** Unlawful use of debit/credit card.
3. Theft of proprietary info: It is an illegal act of obtaining designs, plans, blueprints, codes, computer programs, formulas, trade secrets, graphics, copyrighted material, forms, files, personal or financial info, usually by electronic copying.
4. Denial of service: It is an action(s) that prevents access to a software system by its intended/authorized users or causes delay of its time-critical operations or prevents any part of the system from functioning. It is usually caused by events like **ping attacks, port probes, & excessive amounts of incoming data.**
5. Vandalism or Sabotage: It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, & programs.
6. Computer virus: It is a computer program that can copy itself & infect a computer without permission or knowledge of user.
7. Others: There are several other threats like intrusions, breaches & compromises of respondent's computer networks regardless of whether damage or loss were sustained as a result or not.

4. Write short notes on "Risk Assessment". May 2013
Discuss "Risk Assessment" with the help of "Risk analysis Framework". May 2012

Risk Assessment: It is a step in risk mgt procedure.It determines the quantitative or qualitative value of risk related to a particular situation or threat.It is also termed as a critical step in disaster & BCP since it provides an effective approach that serves as the foundation for avoiding of disasters..
It provides the analysis of threats to resources/assets & determines the amount of protection required to adequately safeguard them, so that the vital systems, operations, & the services can be resumed to normal status in the minimum time in case of a disaster. Thus, risk assessment is a useful technique to assess the risks involved in the event of unavailability of info, to prioritize applications, identify exposures & develop recovery scenarios.
Risk assessment consists of two basic components:
(i) *Data collection*: The data collected in risk assessment should include a comprehensive list of business processes & their resource dependencies.
(ii) *Risk analysis:* Through risk analysis, it is possible to identify, assess, & then mitigate the risk.



5. What do you understand by "Risk Assessment"? Discuss the areas that are to be explored to determine the risk.
What are the areas to be focused upon in Risk Assessment? Nov 2008, Nov 2011, RTP May 2013

Meaning of risk assessment: (Refer Q.No. 4)
The areas to be focused upon are:
1. Prioritization: All applications are inventoried & critical ones are identified. Each of the critical applications is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
2. Identifying critical applications: Amongst the applications currently being processed, the critical applications are identified. Further analysis is done to determine specific jobs in the applications which may be more critical. Even though, the critical value would be determined on the basis of present value, future changes should not be ignored.
3. Assessing their impact on the organization: BCP should not concentrate only on business disruption but should also take into a/c other organizational functions which may be affected **such as** legal liabilities, interruptions of customer services etc.
4. Determining recovery time-frame: Critical recovery time period is the period of time in which, the business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature of operations.
5. Assess insurance coverage:

***"The info system insurance policy should be a multi-peril policy, designed to provide various types of coverage.." Discuss the comprehensive list of items considered for coverage.* Nov 2010**

It may cover the following:
(i) Hardware & facilities: The equipments should be covered adequately. Provision should be made for the replacement of all equipments with a new one by the same vendor.
(ii) Software reconstruction: In addition to the cost of media, programming costs for recreating the software should also be covered.
(iii) Extra expenses: The cost incurred for continuing the operations till the original facility is restored, should also be covered.
(iv) Business interruption: This applies mainly to centres, performing outsourced jobs of the clients. The loss of profit caused by the damaged computer media should be covered.
(v) Valuable paper & records: The actual cost of valuable papers & records stored in the insured premises should be covered.
(vi) Errors & omissions: This coverage is for against the legal liability arising out of errors & omissions committed by system analysts, programmers & other IS personnel.
(vii) Fidelity coverage: This coverage is for acts of employees often in case of financial institutions, which use their own computers for providing services to clients.

(viii) Media transportation: The potential loss or damage to media while being transported to off-site storage should be covered.

6. Identification of exposures & implications: It is not possible to accurately predict as to when & how a disaster would occur. So, it is necessary to estimate the probability & frequency of disaster.

7. Development of recovery plan: The plan should be designed to provide for recovery from total destruction of a site.

6. Define "Risk Management" and also explain the various steps involved in "Risk Management Process".

Risk Mgt.: It is the process of identifying vulnerabilities & threats to the info resources and deciding what countermeasures to be taken to reduce the risk to an acceptable level. Risk mgt encompasses identifying, analyzing, evaluating, treating, monitoring & communicating the impact of risk on IT processes.

Depending on the type of risk & its significance to the business, mgt & the board decides whether to avoid or mitigate or transfer or accept the risk. An organization can also choose to reject risk by ignoring it, which can be dangerous depending upon the type of the project. Normally, IS auditor puts a red flag on such conditions.

Risk Mgt Process: The process of info risk mgt typically involves the following steps:

1. Identifying & classifying the info assets: In this step, the info assets (that support the critical business operations) are identified so that they should be protected.The assets could fall under different groups, which are:

(i) Conceptual/Intangible Assets: These are -

a) **Data & info:** Info stored in various storage devices are subject to unauthorized disclosure, copying, theft, corruption or damage.
b) **Software:** Software like application software & system software are likely to be affected by intentional or unintentional or unauthorized modification by internal or external users or by faulty technology processes.

(ii) Physical/Tangible Assets: i.e People; hardware; networking devices; facilities like AC, dust-free & humidity controlled facilities and documentation like printed forms, manuals, system & database documentation.

2. Valuation of info & info assets as per their criticality: Not all data has the same value. Some data is more valuable such as trade secrets, formulas, & new product info; the loss of such data could create a significant problem for the enterprise by creating public embarrassment or by causing a lack of credibility. On the other side, some info has less impact in the event of its loss, such as a list of customers, details of employees' salaries etc.

Classification of IS resources/assets should be done according to their sensitivity. The assets so identified & grouped may be categorized into different classes, which are:

(i) Top secret: Such info is highly sensitive internal info. **E.g.** Info relating to pending mergers or acquisitions; Investment strategies; plans or designs etc. Disclosure of such info can seriously affect the existence of the organization. Thus, access to such info must be restricted only to a few individuals.

(ii) Secret: Info in this category is strategic to the survival of the organization. Unauthorized disclosure could cause severe damage to the organization & stakeholders.

(iii) Confidential: Info in this category also needs high level of protection but unauthorized disclosure may cause significant loss or damage. Such info is highly sensitive & should be well protected.

(iv) Sensitive: Such info requires higher classification as compared to unclassified info. Disclosure may impact serious impact.

(v) Unclassified: Info that does not fall in any of the above categories finds place in this category. Unauthorized access/disclosure of such info would not cause any adverse impact on the organization.

3. Identifying threats & vulnerabilities to those assets: Threat can be defined as an event which can interrupt or destruct any service, product or process. **Common types of threats are -** Errors, malicious damage/attack, fraud, theft, & equipment/software failure. Threats occur because of vulnerabilities associated with use of info resources. **Examples of vulnerabilities -** Lack of user knowledge, lack of security functionality, poor choice of passwords, & untested technology etc.

These threats could affect the CIA of system info or resources.

(i) Confidentiality: It involves the protection of organization's info from disclosure to unauthorized persons.Threats to confidentiality include intentional as well as unintentional access to sensitive info.

Example of threat to confidentiality - Improper application controls in application software may lead to access of sensitive info by employees.

(ii) Integrity: It requires that the business info & related processes should not suffer any intentional /accidental/unauthorized modification, which may result in serious consequences to the business. Integrity violations may be due to erroneous program codes and system errors which include corruption of files, power failures etc.

Example of threat to integrity: A bank employee not having authority to credit files may temper with the sanctioned amount of credit facilities by bypassing the application controls and making direct changes to data files or by gaining unauthorized access to the manager's login.

(iii) Availability: It ensures the availability of info & IT processes to the authorized users as & when required.

Example of threat to availability: Failure or improper functioning of power system can lead to the abnormal functioning of computer system.

4. Measuring or assessing risk (i.e Info Risk assessment): After identifying the assets & corresponding potential threats, the systems are reviewed for weaknesses that can be exploited & the likelihood of those being exploited. Following types of assessments are done by the info security professional or IS auditor to identify the vulnerabilities or weaknesses:

(i) Vulnerability Assessment: It is the weakness in the safeguards, procedures, technical controls, physical controls or other controls that could be exploited by the threat.

E.g. A hacker may look for the loopholes in the architecture of firewall to compromise the controls & gain unauthorized access to the networks.

(ii) Probability or Likelihood Assessment: It is the estimation of the frequency or the chance of a threat happening. Greater the likelihood of a threat occurring, the greater is the risk. This assessment considers the presence, tenacity, as well as, the

effectiveness of safeguards. The likelihood of occurrence of a threat needs to be reassessed periodically, due to changes occurring in the structure, direction, & environment of an organization.

(iii) Impact Analysis: The threat which is successful in causing harm or loss to an asset results in an impact. Impact may be either in terms of direct loss of money or financial impact such as a hacker stealing a sensitive file containing all the info about credit card customers which is used by the ATM access control system. IT risks can also lead to significant losses such as legal consequences & loss of reputation etc.

5. Developing strategies to manage risks:

What are the major categories of risk mgt strategies? Explain in brief. **RTP May 2013, RTP May 2014**

After the risks have been identified & assessed, appropriate corrections shall be made to the system, if required. The strategies to manage the risk fall into one or more of these four major categories:

(i) Risk Avoidance: i.e not doing an activity that involves risk but it may result in losing out any potential gain that accepting the risk might have provided.

(ii) Risk Mitigation/Reduction: It involves implementing controls to protect IT infrastructure & to reduce the severity of the loss or the likelihood of the loss from occurring. **E.g.** Using an effective anti-virus solution to protect against the risk of viruses.

(iii) Risk Transfer: It involves causing another party to accept the risk i.e sharing risk with partners or insurance coverage.

(iv) Risk Retention/Acceptance: In some cases, it may not be possible to take immediate action to avoid/mitigate the risk. All risks that are not identified or avoided or transferred are retained by default. These risks are called **residual risks.** Risk mgt aims to identify, select & implement the controls that are necessary to reduce residual exposures to acceptable levels.

7. Write short notes on Systematic & Unsystematic risks. **Nov 2013**

Systematic Risks	Unsystematic Risks
These risks remain constant, no matter what technology is used.	These risks are specific to particular technology or application.
These risks are generally dependent on external factors.	These are related to technology & dependent on internal factors.
These risks can be mitigated by *Mgt Process.*	These risks can be mitigated by *Advanced Technology or System.*
The mgt has to incr the cost of risk mitigation to reduce the adverse impact of risks on system or operations.	The mgt issue would be whether additional payment to mitigate the risk is justifiable considering the possibility of loss that may or may not occur.

8. Explain the concept of risk mgt cycle. **June 2009**

It is a process, involving a series of steps. These steps are categorized into three primary functions -

1. Risk Identification/Evaluation: It is important to identify the inherent risk of performing various business functions especially with regard to usage of IT enabled services. Risks can be identified by asking following questions:

- What could go wrong?
- Where are we vulnerable?
- How could someone disrupt our operations?
- What activities are most complex??
- What is our greatest legal exposure?

What are the two primary questions to consider when evaluating the risk inherent in a business function in the context of risk assessment methodologies. Give the purposes of risk evaluation. **May 2010**

The two primary questions to consider when evaluating the risk inherent in a business function are:

(i) What is the probability that things can go wrong? **(Probability)** This view will have to be taken strictly on the technical point of view & should not be mixed up with the past experience.

(ii) What is the cost if what can go wrong does go wrong? **(Exposure)**

What is the purpose of risk evaluation? Give some of the techniques that are available for risk evaluation. **May 2013**

Purpose of Risk Evaluation:

1) Identify the probabilities of failures & threats,
2) Calculate the exposure, i.e., the damage or loss to assets, and
3) Make control recommendations keeping the cost-benefit analysis in mind.

State & explain four commonly used techniques to assess & evaluate risks. **RTP Nov 2012**

Techniques for Risk Evaluation: **June 2009**

A) Judgment & intuition: In many situations, the auditors have to use their judgment & intuition for risk assessment. This mainly depends on the personal & professional experience of the IS auditors & their understanding of the system & its environment.

B) The Delphi approach: {May 2011, RTP Nov 2013, RTP May 2014}

(i) This approach is defined as " a method for structuring a group communication process, so that, the process is effective in allowing a group of individuals as a whole to deal with a complex problem". (ii) This approach was originally developed for the 'US department of defence'. (iii) It was first used by the 'Rand Corporation' for obtaining a consensus opinion. Here, a panel of experts is appointed and each expert gives his/her opinion in writing, in which they enlist the estimate of cost, benefits & the reasons why a particular system should be opted. These estimates are then compiled together. The estimates with pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates to fall within the range. Then a curve is drawn taking all the estimates on the **graph**. The **median** is drawn & this is the consensus opinion.

C) Scoring approach: {RTP May 2014} In this approach, the system risks & their respective exposures are listed. Weights are then assigned to the risk & to the exposures depending on the severity, impact on occurrence, & costs involved. The product of risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk & exposure of the system. System risk & exposure is then ranked to the scores obtained.

D) Quantitative techniques: This technique involves calculating a possible risk impact by multiplying exposure of risk with

probability of risk occurrence. It is the estimation of potential damage in the event of occurrence of unfavorable events, keeping in mind, how often such an event may occur.

E) Qualitative techniques: These techniques are most widely used approaches to risk analysis. Most qualitative risk analysis methodologies make use of a no. of interrelated elements:

- **Threats:** These are the things that can go wrong or that can attack the system. **E.g.** Fire or fraud.
- **Vulnerabilities:** These make a system more prone to attack by threat or make an attack more likely to have some success/impact.
- **Controls:** These are the countermeasures for vulnerabilities. There are four types of controls, that are -

(i) Deterrent controls **(ii)** Preventive controls **(iii)** Corrective controls and **(iv)** Detective controls

2. Risk Assessment: (Refer Q.No. 4)

Following are typical assumptions that can be used during the risk assessment process:

(i) Although impact rating could range b/w 1 & 3 for any facility, rating applied should reflect anticipated, likely or expected impact on each area.

(ii) Each potential threat should be assumed to be "localized" to the facility being rated.

(iii) Although one potential threat could lead to another potential threat, no domino effect should be assumed.

(iv) If the result of the threat would not warrant movement to an alternate site, the impact should be rated no higher than 2.

Risk assessment should be performed in following manner:

The risk assessment should be performed by facility. To measure the potential risks, a **weighted point rating system** can be used. Each level of probability can be assigned points as follows:

Probability	Points
High	10
Medium	5
Low	1

To obtain a weighted risk rating, probability points should be multiplied by the highest impact rating for each facility. Based on rating method, threats that can pose the greatest risk can be identified.

3. Risk Mitigation: It is the systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence. The appropriate risk mitigation measures can be adopted only after analyzing the type & extent of risk.

Explain the common Risk Mitigation Techniques. **Practice Manual, RTP May 2012**
Write short notes on Risk Mitigation Measures. **May 2012**

1) Insurance: Under the scheme of insurance, the risk is transferred from the insured entity to the insurance company in exchange of premium. However, while selecting such an insurance policy, one has to look into the **exclusion clause** to assess the effective coverage of the policy.

2) Outsourcing: The organization may transfer some of the functions to an outside agency & transfer some of the associated risks to that agency. But a careful assessment is required to see whether such outsourcing is transferring the risk or is merely transferring the mgt process.

3) Service Level Agreements: SLA may be entered into with the customers, suppliers, & users. SLA with customers & users may clearly exclude or limit the responsibility of an organization for any loss suffered by the customer & user consequent to the technology failure. **E.g.** A bank may state that services at ATM are subject to availability of service there & customers need to recognise that such availability can't be presumed before claiming the service.

9. Write short notes on "Risk Ranking".

Risk ranking is an important technique to understand the impact of potential threats on IS resources & components. In this approach, the identified risks are ranked based on their impacts. Though the main system i.e the server may be the one with greatest risks but there are many other components & applications which may cause problems. Therefore, risks to these components & applications should also be analyzed & ranked to ascertain the impact of all possible risks.Organizations have to devise their own ranking methods.

For example: The impact can be rated as:

0 = No impact or interruption in operations,
1 = Noticeable impact, interruption in operations for up to 8 hours,
2 = Damage to equipment and/or facilities, interruption in operations for 8 - 48 hours,
3 = Major damage to equipment and/or facilities, interruption in operations for more than 48 hours.

10. What are the considerations in analyzing risks?

These include:

1. Investigating the frequency of particular types of disaster.
2. Determining the degree of predictability of the disaster.
3. Analyzing speed of onset of the disaster.
4. Determining the amount of forewarning associated with the disaster.
5. Estimating the duration of disaster.
6. Considering the impact of a disaster.
7. Identifying the consequences of a disaster.
8. Estimating the potential loss.

11. Write short notes on relationship b/w risks & controls.
In order to achieve goals & objectives, mgt needs to effectively balance risks & controls. Explain in brief.

Risk is the probability that an event or action will adversely affect the organization. In order to achieve the goals & objectives,

mgt needs to effectively balance risks & controls. Therefore, control procedures need to be developed so that they decrease risk to an acceptable level. Risks & controls being out of balance can cause the following problems:

Excessive Risks	Excessive Controls
Loss of assets	Increased bureaucracy
Poor business decisions	Reduced productivity
Non-compliance	Increased complexity
Increased regulations	Increased cycle time
Public scandals	Increase of no value activities

In order to achieve a balance b/w risks & controls, internal controls should be pro-active, value-added, cost-effective & address exposure to risk.

12. Write short notes on relationship b/w IS risks & controls.

IS Risks: Info systems are exposed to many direct & indirect risks. These risks can have significant impact on the business operations. However, through appropriate decisions & actions, these risks can be mitigated but can't be altogether eliminated. Threats to info system can materialize as a result of poor controls or absence of controls.

Controls: A control is a check or restraint on a system, which is designed to enhance its security. Therefore, appropriate controls should be there to minimize the impact of threats to info system. Controls can act to:

- ✓ Reduce a threat,
- ✓ Reduce vulnerability to a threat,
- ✓ Detect an impact,
- ✓ Reduce the impact of a threat, and
- ✓ Recover from an impact.

Understanding the Relationship b/w IS Risks & Controls

It is important for the IS auditor to understand the relationship b/w risks & controls. For this purpose, he should consider the following aspects:

1. He should be thorough with the process of reviewing & evaluating controls.
2. He should be able to evaluate whether available controls are adequate & appropriate to mitigate the IS risks.
3. He should understand that controls always have a cost, but also come with a benefit and it is crucial to balance the cost vs. Benefits of controls.

Example of Costs: Consumption of time, investment of money, & compromising with the performance of systems etc.

Example of Benefits: Risk reduction, Improvement in the effectiveness & efficiency of operations.

13. What are the rules to be applied in determining the use of new controls in the context of IS risks & Controls?

The following rules apply in determining the use of new controls:

1. If controls would reduce risk more than required, then see whether a less expensive alternative exist.
2. If control would cost more than the risk reduction provided, then find something else.
3. If control does not reduce risk sufficiently, then look for more controls or a different controls.
4. If control provides enough risk reduction & is cost-effective also, then use it.

Chapter 6 - Business Continuity Planning & Disaster Recovery Planning

1. What is meant by Business Continuity Plan ? Also explain the areas to be covered by BCP. Nov 2010, RTP May 2013

Meaning of BCP: BCP is the creation & validation of a practical logistical plan which ensure that an organization will recover & restore its partially or completely interrupted critical i.e urgent functions within a predetermined time, after a disaster or extended disruption. The logistical plan is called a BCP. BCP lays out the steps to be initiated on occurrence of a disaster, combating it & returning to normal operations.

BCP covers the following areas:

1. **Business Resumption Planning:** It is a planning that resume the critical business operations at the time of disaster.
2. **Disaster Recovery Planning:** It is an advance planning & preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster such as fire.
3. **Crisis Mgt.:** It is a planning to manage crises events such as network failure.

2. Discuss the Objectives & Goals of BCP. Nov 2008

Objectives of BCP: The primary objective of a BCP is to minimize loss by minimizing the costs associated with disruptions & enable an organization to survive in a disaster & to re-establish its normal business operations. The key objectives of BCP should be to:

(i) Minimize the duration of a serious disaster to business operations;
(ii) Facilitate effective co-ordination of recovery tasks;
(iii) Reduce the complexity of recovery effort;
(iv) Provide for safety & well-being of people on the premises at the time of disaster;
(v) Continue critical business operations;
(vi) Minimize immediate damage & losses.

Goals of BCP: RTP May 2012, Nov 2012, Nov 2013

The goals of BCP should be - to identify weaknesses & implement a disaster prevention program. (+ First 3 objectives are also goals.)

Which aspects should be covered while drafting IS Security Policy for Business Continuity Planning? May 2013
Write short notes on Business Continuity Management. [Topic of chapter 9]

Business Continuity Management: The following are the major aspects, which should be covered while drafting IS 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.

Briefly explain the 'Business Continuity mgt with Controls & Objectives' w.r.t IS policy. [Topic of chapter 8]

A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. This begins by identifying all events that could cause interruptions to business processes and depending on the risk assessment, preparation of a strategy plan. The plan needs to be periodically tested, maintained and re-assessed based on changing circumstances

There is only one control which is described here in below along with its objectives:

- **Aspects of business continuity management:** To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

3. Describe the methodology of developing a BCP. *Practice Manual,* Nov 2008, RTP Nov 2012

The methodology for developing a BCP can be sub-divided into 8 different phases. The extent of each of the phases can be adjusted as per the requirements of particular organization. The methodology emphasis on following:

(i) Providing mgt with a comprehensive understanding of total efforts required to develop & maintain an effective recovery plan;
(ii) Obtaining commitment from mgt to support & participate in the effort;
(iii) Defining recovery requirements from the perspective of business functions;
(iv) Documenting the impact of extended loss to operations & critical business functions;
(v) Focusing on disaster prevention, impact minimization, & orderly recovery;
(vi) Selecting business continuity teams;
(vii) Developing a BCP which is easy to understand, implement, & maintain;
(viii) Integration of BCP into other ongoing business plans, so that it remains viable overtime.

4. Describe the Eight Phases in developing a BCP. *Practice Manual*

1. Pre-Planning Activity: This phase gives an understanding of existing & projected systems environment of the organization that helps to refine the scope of BCP & the associated work. This phase includes the following tasks:

- During this phase, a steering committee should be established that should undertake the overall responsibility for providing direction & guidance to the BCP team. The committee should also make all decisions to the recovery planning efforts;
- The BC manager should work with the steering committee in finalizing the detailed work plan & developing interview schedules for conducting the Security Assessment & Business Impact Analysis.
- *Two other key deliverables are:* To develop a policy to support the recovery program; and To develop/conduct an awareness program to educate mgt & senior individuals who will be required to participate in the BC program.

2. Vulnerability Assessment & definition of Requirement {RTP Nov 2013}: This phase includes the following tasks:

- A thorough security assessment of the system & communication environment; this assessment will enable the BC team to improve any existing emergency plans & disaster prevention measures and to implement required emergency plans & disaster prevention measures where they do not exist.
- To present the findings & recommendations resulting from the activities of Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- Defining the scope of the planning effort.
- Developing a plan framework.
- Assemble BC team & conduct awareness sessions.

3. Business Impact Analysis: It is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. This will cover not just financial loss but also cover some other issues such as reputation loss, regulatory effects etc.

What is the significance of Business Impact Analysis? Enumerate the tasks to be undertaken in this analysis. In what ways the info can be obtained for this analysis? ***Practice Manual,* Nov 2011, May 2013**

A no. of tasks are to be undertaken in this phase are as under:

(i) *Identify organizational risks:* This includes single point of failure & infrastructure risks. Its objective is to identify risks & opportunities and to minimize the potential threats that may lead to disaster.

(ii) Identify critical business processes.

(iii) Identify & quantify threats/risks to critical business processes.

(iv) Identify dependencies & inter-dependencies of critical business processes & the order in which they must be restored.

(v) Determine the maximum allowable downtime for each process.

(vi) Determine the impact to the organization in the event of disaster, e.g. Financial loss, reputation loss etc.

There are a no. of ways to obtain this info; **viz. *Questionnaires, Workshops, Interviews, and Examination of documents***.

The BIA report should be presented to the steering committee. This report identifies critical service functions & the timeframe in which they must be recovered after interruption.

4. Detailed definition of requirements: During this phase, a profile of recovery requirements is developed by identifying resources required to support critical functions identified in phase 3. This profile should include *Hardware, Software, Documentation, Outside Support, Facilities and Personnel* for each business unit.

5. Plan Development: The objective of this phase is to provide timely recovery for all critical processes & their dependencies. The recovery strategies may be two-tiered:

(i) ***Business -*** Logistics, Accounting, Human Resources, etc.

(ii) ***Technical -*** IT

This phase includes the following tasks:

- Defining the recovery plans components,
- Documentation of plans,
- Developing the recovery standards, and
- Developing the organization's recovery strategy needs.

6. Testing the Plan: During this phase, testing/exercising goals are established & alternative testing strategies are evaluated. Unless, the plan is tested on a regular basis, there is no assurance that in the event the plan is activated, the organization will survive a disaster.

Objectives of performing BCP Tests: To ensure that -

- ✓ The recovery procedure are complete & workable.
- ✓ The competence of personnel in performing recovery procedures can be evaluated.
- ✓ The success or failure of BC training program is monitored.

7. Maintenance Program: This refers to change in BCP due to the changes in environment. It is necessary that existing change mgt processes are revised to take recovery plan maintenance into account.

The tasks undertaken in this phase are:

- Determine the responsibility for maintaining the various BCP strategies within the organization,
- Identify the BCP maintenance events to ensure that any organizational, operational, & structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date.
- Implement version control procedures to ensure that the plan is maintained up-to-date.

8. Testing & Implementation: Once the plans are developed, initial tests are conducted & any necessary modifications to the plans are made; the plan is implemented. Specific activities of this phase include the following:

(i) Defining the test purpose/approach; (ii) Identifying test teams; (iii) Structuring the test;
(iv) Conducting the test; (v) Analyzing test results; and (vi) Modifying the plans, as appropriate.

5. Briefly explain the various kinds of Plans that need to be designed for disaster recovery planning.

1. Emergency Plan {*Practice Manual*}: This plan specifies the actions to be undertaken immediately when a disaster occurs. These are:

- Who is to be notified immediately when the disaster occurs - *Mgt., Police, Fire deptt., Medicos, & so on.*
- Actions to be undertaken - *Shutdown of equipment, Removal of files, and Switching-off the power.*
- Evacuation procedures must be specified.
- Return procedures - **e.g.** *Conditions that must be met before the site is considered safe.*

2. Back-up Plan: This plan is intended to restore operations quickly that is why, the info system function continue to service an organization even during the period of disaster. This plan specifies:
(i) The type of backup to be kept, (ii) Frequency with which backup is to be undertaken, (iii) Procedures for making backup,
(iv) Location of backup resources, (v) Site where these resources can be assembled & operations restarted,
(vi) Personnel who are responsible for gathering backup resources & restarting operations, and
(vii) The time frame for recovery of each system.

Resources to be considered for back up while preparing a backup plan:

Resource	*Back up*
Personnel	Training & rotation of duties among IS staff; Arrangement with another company for provision of staff.
Hardware	Arrangement with another company for provision of hardware.
Facilities	Arrangement with another company for provision of facilities.
Documentation	Inventory of documentation stored securely on-site & off-site.
Supplies	Inventory of critical supplies stored securely on-site & off-site with a list of vendors who provide all supplies.
Data/Info.	Inventory of files stored secured on-site & off-site.
Applications S/W	Inventory of application software stored on-site & off-site.
System Software	Inventory of system software stored securely on-site & off-site.

3. Recovery Plan: ***Out of the various plans used in BCP, discuss recovery plan in brief.*** **May 2012**
These plans set out the procedures to restore full info system capabilities. Under this plan, a recovery committee is identified that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee & provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first.

4. Test Plan: The purpose of this plan is to identify the deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization & its personnel for facing a disaster. It specifies the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory.

6. As a system auditor, what control measures will you check to minimize threats, risks & exposures to a computerized system? ***Practice Manual*, Nov 2011**
These control measures are:

Threats/Risks /Exposures	Control Measures
Lack of confidentiality	Use of encryption techniques & digital signature; use of passwords & other authentication techniques; development of a security policy, procedure & standard; employee awareness & training; requiring employees to sign a non-disclosure undertaking; implementation of physical & logical access controls; installation of audit trails ; & audit of confidentiality of data.
Lack of integrity	Use of encryption techniques & digital signatures; Implementation of security policy, procedure & standards; implementation of user identification, authorization & access control techniques; security awareness programs & training of employees; updated antivirus software; backup of system & data security; installation of audit trails, & audit of adequacy of data integrity.
Lack of system availability	Implementation of physical & logical access controls; implementation of system backup procedure; insurance coverage; backup power supply; updated antivirus software; use of passwords & other authentication techniques; security awareness programs & training of employees; installation of audit trails; & audit of adequacy of availability safeguards.
Disgruntled employees	Installation of physical & logical access controls; Installation of one time use passwords; logging & notification of unsuccessful logins; use of disconnect feature on multiple unsuccessful logins; security awareness programs & training of employees; application of motivation theories; job enrichment and job rotation.
Unauthorized users attempt to gain access to the system & system resources	Identification & authentication mechanism such as passwords, biometric recognition devices, tokens; physical & logical access controls; smart cards; disallowing the sharing of passwords; display of warning messages; and regular audit programs.
Hackers & computer crimes	Installation of firewall & intrusion detection systems; frequent change of passwords; installation of one time use passwords; discontinuance of use of installed & vendor installed passwords; use of encryption techniques; use of digital signatures; installation of logging feature & audit trails for sensitive info.
Hostile Software	Establishment of policies regarding sharing & external software usage; updated antivirus software with detection, identification & removal tools; use of diskless PCs & workstations; installation of intrusion detection tools & network filter tools such as firewalls.
Terrorism & industrial espionage	Use of traffic padding & flooding techniques to confuse intruders; use of encryption during program & data storage; installation of intruders detection programs.

7. Write short notes on Single Point of Failure Analysis. ***Practice Manual***
The objective of such analysis is to identify any single point of failure within the organization's infrastructure particularly in the IT infrastructure. Single point of failure have increased due to continued growth in the complexity in the organization's IS

environment. This growth has occurred due to changes in technology & customer's demands for new channels in the delivery service and/or products. Organizations have failed to respond to increase in the exposure from single point of failure by not implementing risk mitigation strategies.

For e.g. One common area of risk from single point of failure is the ***"Telecommunication Infrastructure".*** Because of its transparency, this potential risk is often overlooked. The disaster may occur in an organization due to a single point of failure irrespective of the fact that the resiliency of network (i.e the positive ability of a system to adapt itself to the consequences of a catastrophic failure caused by power outage, fire, bomb etc. particularly in the IT systems) and the mean average failures of communication devices (e.g. *Routers*) have improved.

To ensure single point of failures are identified at the earliest possible time, it is necessary that risk assessment should be performed.

8. Describe the Objectives of Technology Risk Assessment.

The objective of risk assessment are to:

(i) Identify IT risks (ii) Determine the level of risks

(iii) Identify the risk factors (iv) Develop risk mitigation strategies

9. "Technology risk assessment needs to be a mandatory requirement for project to identify single point's failures." - Justify. Describe the benefits of performing a technology risk assessment. Nov 2010, May 2011

Single point of failures have increased due to the continued growth in the complexity in the organization's IS environment. Technology risk assessment is a mandatory requirement to identify single point failures because of the following **benefits**:

(i) To have a business-driven process to identify, quantify & manage risks while detailing failure, suggestions for improvement in technical delivery.

(ii) To have a framework that governs technical choice & delivery processes with cyclic check-points during the project life-cycle.

(iii) Interpretation & communication of potential risk impact & where appropriate, risk reduction to a perceived acceptable level.

(iv) Implementation of strict disciplines for active risk mgt during the project life cycle.

The technology risk assessment ensures that proactive mgt of risks occurs & that no single point of failure is inadvertently built into the overall architecture.

10. Briefly explain the various types of system's backup for the system & data together. Nov 2008, Nov 2011
Discuss various back-up techniques in brief. RTP Nov 2013
Explain briefly the software and data back-up techniques. *Practice Manual*

When the backups are taken of the system & data together, they are called total system's backup. System. **Various backup techniques are described as follows:**

1. Full backup: This is the simplest form of backup with a single restoring session for ***restoring all backed-up files***. Every backup generation contains every file in the backup set. However, the time & space required by such a backup system prevents it from being used for backing up a large amount of data.

2. Incremental backup: This is the faster & more economical type of backup in using the backup space. In this type of backup, only the ***files that have changed since the last full backup*** are backed up again.

3. Differential backup {*Practice Manual*}: This is the most economical method, as only the ***files that have changed since the last full backup/differential backup/or incremental backup*** are backed up.

4. Mirror backup: A mirror backup is most frequently ***used to create an exact copy of the backed up data***. It is identical to a full backup, with the exception that the files are not compressed in zip files & they can't be protected with a password.

11. Discuss the various backup options considered by a security administrator when arranging alternate processing facility. Explain briefly the cold-site, hot-site and warm-site w.r.t BCP/DRP. May 2011, *Practice Manual*

Security administrator should consider the following backup options:

1. Cold site: If an organization can tolerate some down time, then the cold site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system, raised floors, air-conditioning, power, communication lines & so on. An organization can establish its own cold site facility or enter into an agreement with another organization to provide a cold site facility.

2. Hot site: If fast recovery is critical, then an organization might need to have a hot site backup. All hardware & operations facilities will be available at the hot site. In some cases, software, data & supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organizations that have hot site requirements.

3. Warm site: It provides an intermediate level of backup. It has all cold site facilities in addition with hardware that might be difficult to obtain or install. **For e.g.** A warm site might contain selected peripheral equipments plus a small mainframe with sufficient power to handle critical applications in the short run.

4. Reciprocal agreement: Two or more organizations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

12. A company has decided to outsource a third party site for its alternate backup & recovery process. What are the issues to be considered by the security administrator while drafting the contract? May 2010, RTP May 2013

If a third party site is to be used for backup & recovery purposes, security administrators must ensure that a contract is written to cover the following issues:

i. How soon the site will be made available subsequent to a disaster,
ii. The no. of organizations that will be allowed to use the site concurrently in the event of a disaster,
iii. The priority to be given to concurrent users of the site in the event of a common disaster,
iv. The period during which the site can be used,
v. The conditions under which the site can be used,

vi. The facilities & services, the site provider agrees to make available, and
vii. What controls will be in place & working at the off-sit facility.

The above-mentioned are the main issues that should be covered while drafting a contract. These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

13. Having a backup at multiple locations is sometimes essential - Justify.
Write short notes on data back-up redundancy.

1. Multiple back-up media: Important data always requires high protection from being lost. So, it is always desirous to eliminate the single point of failure *such as* failed back-up disk that destroys the entire back-up history should be eliminated.
2. Off-site back-up: Off-site back-up is done to keep at least one copy of redundant backups in an alternate location i.e location other than the working location of the system.
3. Where to keep the back-ups: If removable-media backups are kept next to the computer, a file or other disaster will probably destroy both. A secure off-site location is preferable.
4. Media-Rotation - Tactics: Once in a while, rotate the active backup media (i.e media at working location of system) with one of the offsite stored media. This will update the off-site media with the latest data changes.

14. Briefly explain the types of back-up media.

The most common types of backup media available on the market today include:
1. Floppy Diskettes: These drives provided the cheapest back-up solution earlier. However, these drives have been discontinued today because they were slow & having low storage capacity.
2. DVD Disks: DVD also known as 'Digital Versatile Disc' or 'Digital Video Disc' is a popular optical disc storage media format. Its main uses are video & data storage. They can store more than six times data that can be stored on a CD (i.e Compact Disc).
3. Tape Drives: These drives are also of low cost & their storage capacity is around 4-10 GB. But these drives are relatively slow when compared with other media.
4. Disk Drives: These drives rotate at a very fast speed & have one or more heads that can read & write data.
5. Removable Disks: These disks are very popular for backup of a system. They are quite fast, not much expensive and easy to install & carry around.
6. DAT (Digital Audio Tape) drives: These drives are becoming popular & replacing the tape drives. These tapes come in DLT, SDLT, LTO and AIT format offering up to 260 GB of compressed data.
7. Optical Jukeboxes: They use magnetic optical disks rather than tapes to offer a high capacity backup solution. They are extremely expensive but offer excellent amount of secure storage space, ranging from 5 to 20 terabytes.
8. Autoloader Tape Systems: They use a magazine of tapes to create extended backup volumes. They have a built-in capability of automatically loading or unloading tapes.
9. USB Flash Drives: These drives plug into the USB port and have plug & play capability . They come in various sizes and provides an excellent solution for storing data as a reliable data retention media.
10. Zip Drive: It is a small, portable disk drive used primarily for backing up & archiving personal computer files. It comes into two versions, namely - Parallel and SCSI (i.e small computer system interface).

15. What are the fundamental factors to be considered while selecting the tools & media for backing up the data?

1. Speed: i.e To determine how fast media can be backed up & restored using this media.
2. Reliability: i.e To determine whether the media is reliable, in order to save on costs.
3. Capacity: i.e to determine whether the media is big enough for the firm's backup load.
4. Extensibility: i.e to determine that if the amount of data grows, will the media support this demand.
5. Cost: i.e to determine whether the solution selected by the firm is within its budget.

16. Describe some of the important Back-up tips, which must be kept in mind while taking the backup. RTP May 2012
Describe the general guidelines/tips to be considered for backing-up the data/media.

1. Draw up a simple & easy to understand plan of **'who will do what'** in the case of an emergency.
2. Be organised! Keep record of **'what was backed up, when it was backed up & which backup media contains what data'**.
3. Select the option '*To Verify Backup*', this process will take some time but it ensures that the backup is taken properly.
4. Create a reference point to restore changes.
5. Restrict the restore privilege to the owner/administrator.
6. Use the volume shadow copy (VSS) service in windows server 2003. It allows the user to create point-in-time copies of data so that they can be restored & reverted to at any given time.

17. What are the documentation aspects to be covered in Disaster Recovery Procedural Plan? Nov 2008
Explain the various general components of Disaster Recovery Plan. Nov 2011
What do you understand by the term 'Disaster'? What procedural plan do you suggest for disaster recovery? *Practice Manual*
Describe the contents of disaster recovery and planning document. *Practice Manual*, RTP May 2014

The disaster recovery & planning document may include the following areas:
1. Emergency Procedures: i.e actions to be taken following an incident which endangers business operations & human life.
2. Fallback Procedures: Fallback means an alternative plan which can be used if something goes wrong with the main plan. It describes the actions to be taken to move essential business activities to alternate/temporary locations.
3. Resumption Procedures: It describes the actions to be taken to return to normal business operations.
4. Medical Procedures to be followed in the case of injury.
5. Alternate Manual Procedures to be followed such as preparation of invoices.
6. Insurance papers & claim forms.

7. **Names of employees trained for emergency situation.**
8. **List of phone no. of employees** in the event of an emergency.
9. **Emergency phone list** for fire, police, hardware/software suppliers, customers etc.
10. **List of vendors doing business with organization**, their contact no. & address for emergency purposes.
11. **Responsibilities of individuals** describing '*who is responsible for executing which component of the plan'*.
12. **Awareness & education activities** which are designed to create an understanding of business continuity.

18. "The info system insurance policy should be a multi-peril policy, designed to provide various types of coverage.." Discuss the comprehensive list of items considered for coverage. Nov 2010

It may cover the following:

(i) Hardware & facilities: The equipments should be covered adequately. Provision should be made for the replacement of all equipments with a new one by the same vendor.

(ii) Software reconstruction: In addition to the cost of media, programming costs for recreating the software should also be covered.

(iii) Extra expenses: The cost incurred for continuing the operations till the original facility is restored, should also be covered.

(iv) Business interruption: This applies mainly to centres, performing outsourced jobs of the clients. The loss of profit caused by the damaged computer media should be covered.

(v) Valuable paper & records: The actual cost of valuable papers & records stored in the insured premises should be covered.

(vi) Errors & omissions: This coverage is for against the legal liability arising out of errors & omissions committed by system analysts, programmers & other IS personnel.

(vii) Fidelity coverage: This coverage is for acts of employees often in case of financial institutions, which use their own computers for providing services to clients.

(viii) Media transportation: The potential loss or damage to media while being transported to off-site storage should be covered.

19. Explain the various kinds of Insurance.
Explain briefly the first-party insurances with respect to BCP/DRP. ***Practice Manual***

Insurance is basically divided into two general classes to determine whether the insured is the injured party. Lawyers call these two divisions as *First party & Third party insurance.* **First-party insurance** identifies claims by the policyholder against their own insurance and **Third-party insurance** is designed to protect against claims made against the policyholder & his insurer for wrongs committed by the policyholder. Various kinds of insurance are as follows:

1. First-party insurances - Property Damages: This type of insurance is designed to protect the insured against the loss or destruction of property. It is offered by majority of all insurance firms in the world. Such policies are **also known as *All Risks, Defined Risks, or Casualty Insurance.***

2. First-party insurances - Business Interruption: If an insured company fails to perform its contractual duties, it may be liable to its customers for breach of contract. Reason for not providing the required services might be the loss of info system, data or communications.Such liability can be mitigated by arranging hot sites to occupy in case of fire, flood, earthquake or other natural disaster **OR** by taking out a business interruption policy.

3. Third-party insurance - General Liability: This type of insurance is designed to protect the insured from claims of ***wrongs committed upon others*** (but not written as *By others,* means insured has committed any wrongful act*)*.

E.g. If the insured's computer damages another party's computer, data connectivity, then the insured may be held liable.

4. Third-party insurances - Directors & officers: Directors & officers insurance is a type of Errors & omissions (E & O) insurance. It is designed to protect officers of companies, as individuals, from liability arising from any wrongful acts committed in the course of their duties as officers.

20. What are the 'Types of Testing' to be used under "Testing Methodology" in the context of BCP/DRP.

With good planning, a great deal of disaster recovery testing can be accomplished with moderate (i.e not excessive) expenditure. There are four types of test:

1. Hypothetical: It is a theoretical check to verify the existence of all necessary procedures & actions specified within the recovery plan. It must be conducted regularly.

2. Component: It is the smallest set of instructions within the recovery plan which enables specific processes to be performed. It is designed to verify the detail & accuracy of individual procedures within the recovery plan and can be used when no additional system can be made available for extended periods.

Examples of component test: Backup procedures, offsite tape storage recovery , and security package start-up procedures.

3. Module: It is a combination of components. It aims to verify the validity & functionality of the recovery procedures when multiple components are combined.

Examples of module test: Alternate site activation, system recovery, network recovery, application recovery etc.

4. Full: This test verifies that each component within every module is workable & satisfies the strategy & recovery time objective in the recovery plan. It also verifies the inter-dependencies of various modules to ensure that progression from one module to another can be effected without problem or loss of data.

Objectives of full testing: (i) To confirm that the total time elapsed meets the recovery time objective.
(ii) To prove the efficiency of the recovery plan to ensure a smooth flow from module to module.

21. Briefly explain the 'Testing Methodology' to be used in the context of BCP/DRP.

1. Setting objectives: Before testing a DRP, it is essential to set the objectives of DRP testing. Each test is designed around a worst-case scenario so that all possible disastrous situations could be tested. **Test objectives should include:**

- A fully documented set of procedures to obtain & utilize offsite tapes to restore the system & critical applications to the agreed recovery point, as set out in the recovery plan.

- Fully documented procedures for establishing communication lines/equipment to enable full availability & usage by appropriate areas. **For e.g. -** Business units, data entry, users, etc.
- Detailed documentation on how to restore the production data as stipulated in the recovery plan, to the agreed recovery point.

2. Defining the boundaries: A disaster can impact an organization in several ways. But for practical reasons it is not possible to test a DRP for its far reaching effects. Boundaries are the limits to which test can be extended. **For example -** A test can influence several internal departments and their response can be checked, but it cannot be extended to cover vendor response.
3. Scenarios: The scenario is the description of disaster and its possible consequences.Various scenarios can be simulated for different disasters like fire, earthquake, floods etc and possible effects of such disasters can be visualized.
4. Test criteria: These are the test conditions and their benchmarks which are to be tested. **The role of observer is:**
(i) to give an unbiased view and (ii) to comment on the area of success or (iii) concern to assist in future testing.
5. Assumptions: Certain assumptions are to be made in DRP testing which may relate to conditions existing outside the test boundaries. **For example:**

- All technical info documented in the plan, including appendices, are complete & accurate.
- Purchases from vendor can be made in the specified lead time.
- Tapes & other equipment recalled from offsite are valid & usable..

6. **Test prerequisites:** (i) Before any test is attempted, the recovery plan must be verified as being fully documented in all sections, appendices and attachments.
(ii) Each of the participating teams in the test must be aware of how their role relates to other teams, when & how they are expected to perform their tasks, and what tools are permissible.
(iii) Each team leader is required to keep a log of proceedings for later discussion.
7. Briefing sessions: Before starting the testing activity it is very important to discuss the test modality and implications with the test team. The test team should clearly understand the nature and criticality of test which they are about to perform so that they are not taken by surprise. **Briefing should be done on the following issues:**
(i) Team objectives (ii) Disaster scenario (iii) Time of the test
(iv) Location of each team (v) Assumptions of the test (vi) Restrictions on specific teams
8. Checklists: It provides the minimum issues to be tested and verified during test activity. Checklist is directly related to specific modules of the recovery plan and all sections relevant to particular test must be verified as complete before a test date is set.
9. Analyzing the test: The test output is analyzed to see the effectiveness of the plan and scope for further improvement.
10. Debriefing sessions: After the test has been conducted a meeting of team leaders can be called by the DRP in-charge for discussing the following issues:
(i) Overall performance (ii) Specific team performance (iii) Observations
(iv) Areas of concern (v) Planning for next test (vi) Test reports
11. Test report: The test report will be made consisting of the following:
(i) Executive summery (ii) Objectives (iii) Overall team
(iv) List of actions (v) Conclusions

22. Write short notes on 'Audit Tools & Techniques' used in DRP. RTP Nov 2012, May 2013, RTP May 2014

The best audit tool & technique is a ***periodic simulation of a disaster***. Other audit techniques would include ***Observations, interviews, checklists, inquiries, meetings, and documentation reviews.*** These tools & methods may be categorized as under:
1. Automated Tools: These tools make it possible to review large computer systems for a variety of flaws/mistakes in a short period. They can be used to find threats & vulnerabilities such as *weak access controls, weak passwords, lack of integrity of the system software, etc.*
2. Internal Control Auditing: This includes *Inquiry, observation, and testing.* It helps to detect illegal acts, errors, irregularities or lack of compliance of laws & regulations.
3. Disaster & Security Checklists: A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies & practices.
4. Penetration Testing: It can be used to locate vulnerabilities.

23. What are the elements to be included in the methodology for the development of Disaster Recovery/Business Resumption Plan? Nov 2012

How an auditor will determine whether the DRP was developed using a sound & robust methodology? Explain.Nov 2013

An auditor may determine whether the DRP was developed by using a sound & robust methodology by evaluating the following elements:
(i) Identification & prioritization of the activities which are essential to continue functioning.
(ii) Determining that the plan is based upon a BIA that considers the impact of the loss of essential functions.
(iii) Determining that the operations managers & key employees participated in the development of the plan.
(iv) Determining that the plan identifies the resources that will likely be required for recovery & the location of their availability.
(v) Determining that the plan is simple & easily understood so that it will be effective when it is required.
(vi) Determining that the plan is realistic in its assumptions.

24. How an auditor will determine whether the DRP/BRP include the 'Provisions of personnel'? Explain.

In this regard, the auditor may determine the following aspects:
(i) Whether the plan has a provision for replacement staff, when necessary?
(ii) Whether the plan includes provisions for people with special needs?
(iii) Whether the plan includes contact info of key employees, especially after working hours?
(iv) Whether the key employees have seen the plan, and are all employees aware that there is such a plan?
(v) Whether the employees have been told about their specific roles & responsibilities in case plan is put into effect?

25. How an auditor will determine whether the DRP/BRP cover the 'Aspects relating to building, utilities & transportation'?

In this regard, the auditor may determine the following aspects:

(i) Whether the plan has a provision for having a building engineer to inspect the building & facilities soon after a disaster so that the damage can be identified & repaired to make the premises safe for the return of employees as soon as possible.

(ii) Whether the plan considers the need for alternative shelter, if required?

(iii) Whether the plan considers the failure of electrical power, natural gas, toxic chemical containers, & pipes?

(iv) Whether the plan considers the disruption of transportation systems?

(v) Verify that the backup facilities are adequate based on projected needs.

26. How an auditor will determine whether the DRP/BRP cover the 'aspects relating to IT environment'?

In this regard, the auditor may determine the following aspects:

(i) Whether the plan reflects the current IT environment?

(ii) Whether the plan includes prioritization of critical applications & systems?

(iii) Whether the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable?

(iv) Whether the plan include arrangements for emergency telecommunications?

(v) Whether there is a plan for alternate means of data transmission in case the computer network is interrupted?

27. How an auditor will determine whether the DRP/BRP cover the 'aspects relating to Administrative Procedures'?

In this regard, the auditor may determine the following aspects:

(i) Does the DRP/BRP cover administrative & mgt aspects in addition to operations?

(ii) Is there a designated emergency operations center where incident mgt teams can coordinate response & recovery?

(iii) Whether it covers procedures for disaster declaration, general shutdown & mitigation of operations to the backup facility?

(iv) Have essential records been identified?

(v) To facilitate retrieval, are essential records separated from those that will not be required immediately?

Chapter 7 - An Overview of ERP

1. Define ERP.

An ERP system is a fully integrated business mgt system covering functional areas of an enterprise like Logistics, production, finance, Accounting & human resources. It organizes & integrates operation processes & info flows to make optimum use of resources such as men, material, money & machine. ERP is a global, tightly integrated closed loop business solution package and is multifaceted. ERP promises one database, one application and one user-interface for the entire enterprise.

2. Bring out the Evolution of ERP. **May 2002**

ERP is evolved through improvements in other IS. Improvements in other IS are required due to following reasons:

- Aggressive cost control initiatives
- Need to analyze costs/revenues on a product or customer basis
- Flexibility to respond to changing business requirements
- More informed mgt decision-making
- Changes in ways of doing business.

These improvement requirements in IS has given different types of IS over the years. They are:

(i) Management Info system (MIS)
(ii) Material Resource Planning (MRP)
(iii) Manufacturing Resource Planning (MRP II)
(iv) Money Resource Planning (MRP III)
(v) Integrated Info system (IIS)
(vi) Executive Info system (EIS)
(vii) Enterprise-wide Info System (EWS)
(viii) Corporate Info system (CIS)

ERP has evolved from the system known as MRP II with the integration of info b/w vendor, customer & manufacturer using networks such as LAN, WAN and INTERNET etc. MRP II is a method of planning of all the resources of the mfg co. It involves all operational& financial planning and has simulation capabilities to answer "WHAT IF" questions. However, MRP II has a no. of drawbacks. The main problem is that it has not been able to effectively integrate the different functional areas to share the resources effectively.

The major drawback of MRP II gave rise to ERP system. ERP system provides an integrated info storehouse where info needs to be stored only once and can be further processed & reported to anyone in the value chain. ERP brings together in one platform different business functions, procedures, ideologies etc to make business functions more effective.

3. Outline the Technology required for ERP Or Describe how enabling technology helps in ERP Evolution.

It is not possible to think of an ERP system without sophisticated IT infrastructure. It is said that the earlier ERP systems were built only to work with huge mainframe computers. The new Era of PC, Advent of Client-Server technology and Relational DBMS, all have contributed for the ease of deployment of ERP systems. ERP uses the latest technologies available in the market to provide most efficient IS. The most important technology which enables ERP system to work efficiently is the Client-Server technology.

Client-Server Technology [Nov 2011] - Most of the ERP systems exploit the power of Three-tier Client-Server Architecture. In a client-server environment, data is stored on back-end database server and application logic/business rules are stored on middle ware and presentation for data entry & outputs is kept at client workstation.

ERP uses many other technologies for an integrated & efficient IS. **For Example -** Data Mining, Data Warehousing, Work-group flow, Internet, Intranet and EDI etc.

4. Any system has to possess few Characteristics to qualify for a true ERP solution. What are they? **Nov 2008; Nov 2012;RTP Nov 2013; RTP May 2014**

An ERP system is not only the integration of various organization processes. Any system has to possess few characteristics to qualify for a true ERP solution. These features are:

(i) Flexible - ERP system should cover different languages, currencies & accounting standards etc and it should be flexible to respond to the changing needs of an organization. The client-server technology enables ERP to run across various database back ends through open database connectivity (ODBC).

(ii) Modular & Open - ERP system has to have open system architecture i.e. it implies that any module can be interfaced or detached, whenever required, without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.

(iii) Comprehensive i.e. it should be able to support variety of organizational functions & must be suitable for a wide range of business organizations.

(iv) Beyond the Company i.e. it should not be confined to the organizational boundaries rather it should also support online connectivity to other business entities of the organization.

(v) Best Business Practices i.e. it must have a collection of the best business processes applicable worldwide.

5. What are the Features of an ERP? **Nov 2009**
Will you suggest ERP solution to overcome the problems? If yes, explain why? **Nov 2011**

Following are the reasons for ERP implementation:

(i) ERP provides Multi-platform, **Multi-facility**, Multi-code mfg, Multi-currency & Multi-lingual facilities.

(ii) It has **End-To-End Supply Chain Mgt (SCM)** to optimize the overall demand & supply of data.

(iii) It facilitates **Organization-wide integrated info system** covering all functional areas like production, marketing, finance and accounting & human resources.

(iv) It bridges the info gap **across organizations.**

(v) It provides complete integration of systems not only across departments but also **across companies** under the same mgt.

(vi) It allows **automatic introduction of latest technologies** like EFT, EDI, and E-Commerce etc.

(vii) It **provides intelligent business tools** like DSS, EIS to enable better decision-making.

(viii) It **eliminates most of the business problems** like material shortages, quality mgt, cash mgt , inventory mgt etc.

(ix) It performs core activities & increases customer services thereby **increasing corporate image.**

6. Describe the various business processes which can be integrated using ERP. {Chapter 1 Que} Nov 2013

Ans. 1. **Business system:** It includes
(i) Business forecasting for product /mkt groups (ii) Target fixing & allocation by key parameters
(iii) Strategy formulation & implementation (iv) Resource allocation to key result areas
(v) Strategy monitoring & control (vi) Info-based mgt for mgt applications
2. **Production:** It includes
(i) Production planning & control (ii) Purchasing & procurement system (iii) Inventory mgt
(iv) Inventory analysis & valuation (v) Excise/Custom interface (vi) Production info systems for production applications
3. **Maintenance:** It includes
(i) Plant maintenance planning (ii) Breakdown, preventive & conditional maintenance
(iii) Monitoring performance of maintenance action (iv) Maintenance info systems for maintenance applications
4. **Quality Control:** It includes
(i) Quality assessment against standards (ii) Quality assessment by process, material & work center location
(iii) Analysis of quality by reasons & actions taken (iv) Quality control info systems for quality control applications
5. **Marketing:** It includes
(i) Mkt/Product/Customer analysis (ii) Sales forecasting & Budgeting (iii) Mkt Research info
(iv) Distribution & channel mgt (v) Order processing & analysis (vi) Marketing info systems for marketing applications
6. **Finance:** It includes
(i) Financial planning & control (ii) Mgt of long-term funds & working capital mgt
(iii) Ledgers, payables & receivables (iv) Finance info systems for finance applications

7. Why Companies undertake ERP? OR If you are the CEO of the company, what factors would be considered before undertaking implementation of ERP system? May 2010

1. Integrate Financial Info: As the CEO tries to understand the company's overall performance, he may find many different versions of truth.
For Example - Finance has its own set of revenue numbers; Sales has another version; and the different business units may each have their own version of how much they contributed to revenue.
ERP creates a single version of truth that can not be questioned because everyone is using the same system.
2. **Integrate Customer Order Info:** By having the info in one software system rather than scattered in many different systems, companies can keep track of customers orders more easily, and coordinate manufacturing, inventory & shipping among many different locations simultaneously.
3. **Standardize & speed up mfg processes:** ERP systems come with standard methods for automating some of the steps of a mfg process. Standardizing those processes & using a single integrated system can save time, increase productivity & reduce headcount.
4. **Reduce Inventory:** ERP helps the mfg process flow smoothly & it improves the visibility of order fulfillment process inside the company, which can lead to reduced inventories of raw materials & finished products at the warehouses & shipping docks.
5. Standardize HR info: ERP provides a simple method for tracking employees' time & communicating with them about benefits & services.

8. What are the pre-requisites for (or challenges in) successful ERP implementation? RTP Nov 2002
How will you get over the impediments for the successful implementation of ERP? Mention any five. May 2010

ERP implementation is a risky effort since it involves considerable amount of time, efforts & valuable resources. Even with all these, the success of an organization is not guaranteed. Following are the pre-requisites for successful ERP implementation:
1. The success of an implementation mainly depends on how closely the implementation consultants, users & vendors work together to achieve the overall objectives of the organization. The implementation consultants have to understand the needs of users, understand the prevailing business realties & design the business solutions keeping in mind all these factors. It is the users who will be driving the implementation & therefore their active involvement at all stages of implementation is vital for overall success of implementation.
2. ERP is an enabling tool which makes one do his work better which naturally need additional efforts.
3. During the course of implementation, the standard package may undergo changes which may be simple one or a major 'functionality' change. The package should be expandable & adaptable to meet these changes.
4. Any change in one functional module will have an adverse impact on the functioning of the other modules of the package. Maximum benefit will be available only when the standard package is implemented in totality.
5. The roles & responsibilities of the employees have to be clearly identified, understood & configured in the system. The employees will have to accept new processes & procedures laid down in the ERP system.
6. The implemented ERP package must give a good return on investment.

9. What are the benefits of using ERP System? {Chapter 1 Que} Nov 2011, RTP May 2014

1. **Better use of Organizational Resources:** ERP enables an organization to make better use of its resources which are scarce by their nature. Making better use of these resources is possible because ERP offers a model which indicates where the resources find best usage & how resources can be managed to produce the best result. Thus, through the application of ERP, organizational resources are put at a place where they have their optimum utilization.
2. **Lower operating costs:** ERP results into lower operating costs to the organization. It is possible due to improved business performance through cycle time reduction, inventory reduction, order fulfillment improvement etc. Lower operating cost means improved profitability for the organization.

3. **Proactive decision-making:** A proactive decision-making process emphasis that decisions must be made in advance of likely environmental changes & anticipated competitive moves by competitors.
4. **Decentralized decision-making:** ERP enables an organization to decentralize its decision-making process. Thus, decisions are made at those points at which these are relevant for execution. Due to faster processing technology & SQL, managers can see the info in their own perspective. Further, with intelligent ERP downloads, decisions can be made even at lower mgt levels. Thereby, releasing the burden on higher mgt levels & freeing them for strategic thinking.
5. **Flexibility in business operations:** An organization has to design its business operations according to changing environmental needs. In order to take care of changing environmental needs, ERP provides flexibility in business operations because different languages, currencies, accounting standards etc can be covered in one system.
6. **Enhanced customer satisfaction:** To compete effectively in today's marketplace, organizations must focus on their customers. Customers have become increasingly aggressive in demanding quality & service because they have a wide range of choices. ERP provides the way foe efficient & effective processing of customers' requests & emphasizing customer relationship mgt.

Describe the key Benefits of ERP, in brief. (i.e Benefits of implementing ERP packages) RTP May 2014

The benefits that can be achieved by implementing ERP packages are as follows:
(i) ERP packages make the best use of various resources;
(ii) They reduce paper documents by providing on-line formats for quickly entering and retrieving information;
(iii) They improve timeliness of information by permitting posting daily instead of monthly;
(iv) They provide greater accuracy of information with detailed content, better presentation, satisfactory for the auditors;
(v) They facilitate improved cost control;
(vi) They provide faster response and follow-.up on customers;
(vii) They facilitate more efficient cash collection;
(viii) Better monitoring and quicker resolution of queries;
(ix) Enables quick response to change in business operations and market conditions;
(x) They help to achieve competitive advantage by improving its business process;
(xi) They improve supply-demand linkage with remote locations and branches in different countries;
(xii) They provide a unified customer database usable by all applications;
(xiii) They improve International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages;
(xiv) They improve information access and management throughout the enterprise;
(xv) They provide solution for problems like Y2K and Single Monetary Unit (SMU) or Euro Currency.

10. What are the limitations of ERP systems? {Chapter 1 Que}

(i) An ERP system provides current status only But managers may also require past info to identify trends & patterns for better decision making.
(ii) The methods used in ERP applications are not integrated with other organizational or divisional systems. Further, they do not include external intelligence.
(iii) ERP systems may be too time consuming & costly for certain organizations.

11. What key planning & implementation decisions are taken for ERP implementation?

1. ERP or Not to ERP?

Decision to implement an ERP should be based on following factors:
(i) Technology i.e. (a) Need to integrate the functions of individual systems; (b) Replace poor-quality existing systems; and (c) merge acquisitions with new capabilities into the business environment.
(ii) Process Improvements i.e. actions that result in personnel & IT cost reductions.
(iii) Productivity Improvements i.e. (a) The need to close the financial cycle; and (b) Increase the overall production from an enterprise viewpoint.
(iv) Strategic Considerations i.e. (a) To implement new strategies not supported by the current software; (b) To improve customer service & satisfaction; and (c) To enhance customer responsiveness.

2. Follow Software's processes or Customize?

This key decision may determine the success or failure of the ERP effort.

Follow software's processes	Customization
Merits: If the organization decides to follow the process of software, this will result in the organization following best practices within its sector, thereby giving it a chance to improve & standardize their processes. This approach will also facilitate future change to the ERP software. **Demerits:** This approach can create significant turmoil (i.e. confusion/resistance/misunderstanding/disorder) by requiring the employees to change their ways of doing business.	**Merits:** If the organization decides to stick with its current processes & customize the software to fit these processes, the organization obviously will not have to experience the pain & stress associated with changing its process. **Demerits:** It will be very costly to customize & maintained the software over time. Interfaces modular compatibility needs to be sustained.

3. In-house or Outsource?

In-house	Outsource
Merits: (i) A better match b/w the software & the business; (ii) Applications optimized for the organization; and (iii) Better maintained security. **Demerits:** An in-house approach can't be accomplished if there is a lack of internal expertise & personnel to support such an	**Merits:** It allows the organization to continue to focus on its core mission, avoid a relative substantial financial commitment & minimize the impact on the MIS department. **Demerits:** It provides opportunities to the external people to affect the employees' morale & give rise to security issues.

effort.	

4. "Big Bang" or Phased Implementation?

Big Bang Implementation	Phased Implementation
It involves having all modules at all locations implemented at the same time. **Characteristics:** (i) No need for temporary interfaces; (ii) Limited requirement to maintain legacy software; (iii) Cross-module functionality; and (iv) Low overall cost if no contingencies arise.	In phased implementation, the modules are implemented in phases, often at a single location at a time. **Benefits:** (i) Smoothing of resource requirements; (ii) Ability to focus on a particular module; (iii) Availability of existing legacy systems as a fall-back; (iv) The knowledge gained with each phase & the usefulness of demonstrable working system.

5. The wave approach: This approach involves the application of different waves of change to different business units or regions.

6. Parallel implementation: This approach involves both ERP & an existing system running together for a period of time.

Merits	Demerits
(i) This approach provides a basis of comparison. (ii) Existing system serves as backup.	(i) It requires more computing & human resources; so,it is costly. (ii) Existing system may not be properly maintained.

7. Instant cutovers (flip-the-switch):

Merits	Demerits
(i) This approach is lower in cost, so it motivates the users to seriously convert to the new system. (ii) This approach reduces the need for redundant systems.	This approach tends to be risky, stressful to users and requires a high level of contingency planning.

12. Explain the steps involved in implementation of a typical ERP package. June 09; RTP Nov 12; RTP Nov 13 & May 14
Explain the ERP implementation Methodology

Several steps are involved in the implementation of a typical ERP package. These are:

(i) **Identifying the needs for implementing an ERP package:** Some of the basic questions to be answered are:
- Why should an ERP package be implemented?
- Will it improve profitability?
- How does it improve customer satisfaction?
- Will it help to reduce product-cost?
- How can it help to increase business turnover?

(ii) **Evaluating the 'As is' situation of the business** i.e. to understand the strength & weakness prevailing under the existing circumstances. For this purpose, the various functions should first be listed, which may:
- Total time taken by the business processes;
- No. Of decision points existing in the present scenario;
- No. Of departments/locations of business processes;
- The flow of info & its routing;
- The no. Of reporting points currently available.

(iii) **Deciding the 'Would be' situation for the business** i.e. the changes expected after the implementation of ERP. The concept of 'Benchmarking' is used to see that the processes achieved are the best in industry. Benchmarking is done on various factors like cost, quality, service etc.

(iv) **Re-engineering the business process:** This process is done to achieve the desired results in the existing processes by way of
- Reducing the business process cycle time;
- Reducing the no. Of decision points to a minimum; and
- Making the flow of info more efficient & eliminating the unwanted flow of info.

(v) **Evaluating the various available ERP packages to assess suitability**. (Refer Q.No. 14)

(vi) **Finalizing the most suitable ERP package for implementation:** This is done by making a comparison of critical factors through a matrix analysis.

(vii) **Installing the required hardware & networks for the selected ERP package:** This work is carried out in a phased manner depending on the schedule of implementation & the need of hardware components.

(viii) **Finalizing the implementation consultants who will assist in implementation:** factors of selection for consultants are:
(a) Skill set (b) Industry specific experience (c) Cost of hiring the consultant

(ix) **Implementing the ERP package:** The general steps involved in the implementation are:
(a) Formation of team
(b) Preparation of plan
(c) Mapping of business processes to package
(d) Gap analysis
(e) Customization
(f) Uploading of data from existing system
(g) Test runs
(h) Parallel run
(i) User training
(j) Concurrence fro user
(k) Migration to new system
(l) User documentation
(m) Post-implementation support
(n) System monitoring & fine tuning

13. for the Selection of ERP package, state the issues to be considered. June 2009

While selecting the ERP package, the performance of following issues should be taken into account:
(i) Better inventory management and control;
(ii) Improved financial reporting and control;
(iii) Automation of certain tasks;
(iv) Improved production planning;
(v) Better information on stocks at various locations;
(vi) More accurate costing of products;
(vii) Better credit control;
(viii) Improved cash flow planning;
(ix) Automatic quality control and tracking;
(x) Better after sales services;
(xi) Better information and reporting to top mgt.

14. Why does an organization implement an ERP package and evaluate the various available ERP packages for assessing suitability? Mention the various evaluation criteria that are required to assess the suitability of ERP package on implementation. May 2009; Nov 2010

Reasons for implementation of ERP package: ERP implementation in the organization brings together in one platform different business functions, different personalities, procedures, ideologies & philosophies with an aim to pool knowledge base to effectively integrate & bring worthwhile & beneficial changes in the organization.

Reasons why an organization does evaluation of various available ERP packages for assessing suitability:

(i) Implementation of ERP is a risky effort since it involves considerable amount of time, efforts & valuable resources. Even with all these, the success of an implementation is not guaranteed.

(ii) The ability of ERP package to manage & support dynamically changing business process is a critical requirement for the organization and therefore, the package should be expandable & adaptable to meet these changes.

(iii) The ERP implementation methodology involves several steps, of which, one is evaluating the various available ERP packages to assess suitability.

Criteria for evaluation of various ERP packages: Evaluation of ERP packages are done based on the following criteria -

1. Flexibility: (i) ERP package should enable the organizations to respond quickly to changing environment; and

(ii) Allows the organization to concentrate on new products & markets.

2. Comprehensive: (i) ERP package should be applicable across all sizes, functions & industries.

(ii) It should have in-depth features in -

(a) Accounting & Controlling; (d) Sales & distribution;

(b) Production & material mgt; (e) Human resource mgt (HRM); and

(c) Quality mgt & plant maintenance; (f) Project mgt

(iii) It should also have info & early warning systems for each function and enterprise-wide business intelligence system for informed decision-making at all levels.

(iv) It should be open & modular.

3. **Integrated:** ERP package should integrate the functions like sales & material planning, production planning, warehouse mgt, financial accounting, and HRM; thereby enabling the knowledge workers to receive the right info & documents at the right time.

4. **Beyond the company:** ERP package should support & enable inter-enterprise business processes with customers, suppliers, bank, govt & business partners and create complete logistical chain **covering** the entire route from supply to delivery; multiple geographies, currencies & country specific business rules.

5. **Best business practices:** The software should enable integration of all business operation in an overall system & should include the best business practices that reflect the experiences, suggestions & requirements of leading companies across industries.

6. **New Technologies:** ERP package should incorporate cutting-edge & future-proof technologies such as object orientation into product development and ensure inter-operability (i.e. able to be operated) with internet & emerging technologies.

7. **Other Factors to be considered:**

(i) Global presence of package (v) Obsolescence of package

(ii) Local presence (vi) Ease of implementation of package

(iii) Mkt targeted by the package (vii) Cost of implementation

(iv) Price of package (viii) Post-implementation support availability

15. Write down the guidelines which are to be followed before starting the implementation of an ERP package. RTP Nov 2012; RTP May 2013; May 2013

There are certain general guidelines which are to be followed before starting the implementation of ERP package. These are:-

- ✓ Understanding corporate needs & culture of organization & then adopt the implementation techniques to match these factors;
- ✓ Doing a BPR exercise prior to starting the implementation;
- ✓ Establishing a good communication network across the organization;
- ✓ Providing a strong & effective leadership so that people down the line are well motivated;
- ✓ Finding an efficient & 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;
- ✓ Adapting the new system & making required changes in the working environment to make effective use of system in future.

16. What are the Expectations & Fears of mgt during Post-Implementation of ERP/Explain Post-implementation Scenario

These are the scenarios which emerge after ERP implementation but these start coming in the mind of mgt & start at the time of ERP implementation. These scenarios start emerging in the form of "Expectations & Fears".

Expectations	Fears
➢ An improvement in processes. ➢ Increased productivity on all fronts. ➢ Total automation & disbanding of all manual processes. ➢ Elimination of all manual record-keeping. ➢ Improvement of all KPIs. ➢ Real-time info systems available to concerned people on need basis. ➢ Total integration of all operations.	➢ Job redundancy ➢ Loss of importance (as info is no longer an individual prerogative/custody). ➢ Change in job profile. ➢ Increased stress caused by greater transparency. ➢ Individual fear of loss of authority. ➢ An organizational fear of loss of proper control & authorization.

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

17. Identify the Risks & Governance issues, an org'n faces while migrating to an integrated ERP system? RTP May 14
ABC limited had recently migrated to real-time integrated ERP system, As an IS auditor, advice the company as to what kinds of business risks it can face? Nov 2009; May 2011; RTP May 2012; RTP May 2013
Write short notes on reasons for failure of ERP projects. May 2013

Organizations face several new business risks when they migrate to real-time, integrated ERP systems. Those risks include:

1. Single sign on: Advantage - It reduces the security administration effort associated with administrating web-based access to multiple systems. **Disadvantage -** This feature introduces an additional risk i.e. an incorrect assignment of access may result in inappropriate access to multiple systems.

2. Single point of failure: Since all the organization's data & transaction processing is within one application system, failure to that system (which is ERP's main server) may bring down the working of entire organization info system.

3. Structural changes: Significant structural changes relating to personnel & organization may be associated with re-engineering or re-designing business processes, for which, there is a risk of non-acceptance and incompatibility.

4. Change management: ERP implementation not only requires the implementation of computer based integrated system but also requires changes in existing processes, culture & working methods of organization's staff or stakeholders. Therefore, adapting to new processes, culture & working methods for staff is always a big challenge.

5. Job role changes: The change mgt & structural changes may require the change in job profiles of staff. Here, risk is that the staff often resist for change in their job profiles.

6. Distributed computing experience: ERP provides a distributed data processing system which helps to process data from anywhere. Inexperience with implementing & managing distributed computing technology may create significant challenges.

7. Increased system access: Increased remote access by users & outsiders and high integration among application functions may allow increased access to application & data.

8. Dependency on external assistance: Organizations may sometimes require external assistance. Unless such external assistance is properly managed, it could introduce security & resource mgt risk that may expose the organizations to greater risks.

9. Audit Expertise: The complexity of ERP systems has created specialization such that each specialist may know only a small fraction of entire ERP's functionality in a particular core module. Therefore, specialist expertise is required to effectively audit & control an ERP environment.

10. Privacy & Confidentiality: There is a risk of disclosure of personal confidential info to greater extent as ERP systems are connected with multiple external data sources.

18. Why do ERP projects fail so often?

ERP is a set of best practices for performing the various duties in an organization that may be related to finance, mfg or warehouse etc. But due to some reasons ERP projects fail so often. These reasons may be as under:

1. **Resistance to change:** To obtain the maximum benefit from ERP, there must be cooperation from staff. But, if the staff using ERP in indifferent departments does not agree that the working methods embedded in ERP are better than those they are currently using, they will then resist using the software or they will demand the IT department to change the software to match the ways they currently using.
2. **Inability to manage advance technology of ERP:** To make the ERP software compatible to the existing ways of doing work, the IT department customizes the software. Customization may make the software more unstable & harder to maintain. This may cause ERP project to break down.

19. How does ERP fit with e-commerce?

ERP fits with e-commerce due to following reasons:

- ✓ Today, customers & suppliers demand access to the same info that an organization's employees require through ERP system.
- ✓ E-commerce means IT departments need to build two new channels of access into ERP systems viz. One for customers known as B2C and one for suppliers & partners known as B2B. These two audiences want two different types of info from one ERP system. Consumers want order status & billing info; and Suppliers & partners want just about everything else.

However, companies with e-commerce ambitions face a lot of hard integration work to make their ERP systems available over the internet. Thus, the integration of ERP & E-commerce requires careful planning.

20. How will you establish & implement Critical Success Factors (CSFs) & Key Performance Indicators (KPIs) in an organization, for achieving the benefits of implementation of ERP? May 2007
Explain the Concept of (a) CSFs, (b) Performance measures, and (c) KPIs
Explain the life of ERP after implementation.

Effective use of ERP is a direct result of steps taken at the time of implementation toward preparing the organization. Change integration has to be necessarily embedded in the **task list** for any ERP implementation. The main tool for this is the **process of communication** in all forms that are - written, oral, workshops, meetings etc. The process should start quite early by educating all layers of the mgt on the particular ERP product, its relevant functionality, limitations & benefits.

Critical Success Factors (CSFs): CSF is a factor that is critical in the success of an organization working. CSFs vary from industry to industry. The company should continuously evaluate its CSFs against KPI/Benchmark.

E.g. Time taken to handle a particular customer complains is a CSF.

From these CSFs, **Performance measures** required to address these CSFs should be selected.

Key Performance Indicators (KPIs): The numeric figures against performance measures can be classified as KPIs. KPI may vary from company to company or country to country and in some cases, KPI may not be available. Therefore, the company should select appropriate KPI for their CSF evaluation.

21. What are the post-implementation blues/problems/difficulties in ERP systems? Also list measures to overcome these Problems. OR

You are entrusted with the duty of implementing ERP in your office. You have taken care of all the preparation during implementation. However, during post-implementation, there will be need for course correction many times. What can be reasons for them? Nov 2010

The need for course correction during post-implementation of ERP may be because of the following reasons:
(i) A change in the business environment requires a change in the CSFs resulting in a new or changed set of KPI necessitating re-configuration.
(ii) A review indicates a need for change in some processes.
(iii) Vision changes in the ERP & improvements in hardware & communication technology necessitate changes.
(iv) New additions to the business require extra functionality.

22. What are the tasks for which the company should be ready for post-implementation period of an ERP system? May 2011

Having evolved the processes while the configuration, construction & implementation are in progress, the organization needs to ready itself for the post-implementation period. Some of the tasks that are to be performed are to:
(i) Develop the new job descriptions & organization structure to suit the post ERP scenario;
(ii) Determine the skill gap between existing jobs & envisioned jobs;
(iii) Assess training requirements and create & implement a training plan;
(iv) Develop & amend HR, financial & operational policies to suit the future ERP implementation; and
(v) Develop a plan for workforce logistics adjustment.

23. List a few ERP vendors and briefly discuss the ERP packages offered by them. May 2012

There are a few ERP packages available in the mkt these days. Some of these are developed indigenously also. However, these indigenous packages may not be able to compete with the global ERP packages in terms of functionality & coverage of business segments & scale. Some of the global packages along with the vendors are listed below:
1. **Baan (The Baan Company) :** "Baan" was initially developed for an aircraft company "Boing" in nineties and it was subsequently launched as a generalized package in 1994.It offers sound technology & coverage of broad functional scope. It offers credible tools for business process analysis linked to implementation of its software.
2. **Business Planning & Control System (BPCS):** It targets only mfg companies. It offers strong functionality for discrete & Kanban mfg. However,it lags in process oriented implementation tools & workflow.
3. **Mapics XA (Marcam Corporation):** Mapics is a suite of 40 modules with good enough functionality. It offers robustness, easy implementation & reasonable value for money. Many users viewed it as a legacy application.
4. **MFG/Pro (QAD):** This package is strong in repetitive mfg; originally designed to meet MRP II standards. It offers reliable mfg functionality & straight forward implementation.
5. **Oracle Applications (Oracle):** It gives internet-enabled, network-centric computing. It also offers database, tools, implementation, applications & UNIX operating systems under one stop-shop umbrella. It is currently running on wide choice of hardware.
6. **R/3 (SAP):** It is a mkt leader with excellent philosophy of matching business processes with its modules. It covers almost all business segments.
7. **Systems 21 (JBA):** Its software license revenues are small compared to other major ERP vendors. It offers strong attractive features, reliable mfg solution.

24. What is meant by Business Process Re-engineering? RTP Nov 2004

(i) According to Hammer & Champhy ; "BPR is the fundamental re-thinking & radical re-design of processes to achieve dramatic improvement in critical, contemporary measures of performance such as cost, quality, service & speed."
(ii) Radical re-design means BPR is re-inventing & not enhancing or improving. In a nutshell, BPR approach says that "whatever you were doing in past is all wrong", do not get biased by it or reassemble your new system to redesign it afresh.
(iii) Fundamental rethinking means asking the questions "why do you do what you do", thereby eliminating business process altogether if it does not add any value to the customer.
(iv) The business objectives of an enterprise viz. Profits, customer-satisfaction through optimal cost, quality, deliveries etc are achieved by **transformation of business processes** which may or may not require the use of IT.
(v) Thus, BPR aims at transformation of business processes to achieve dramatic improvement.

25. Write short notes on Business Engineering. Nov 2010,Nov2012

(i) **BE** has come out of merging of two concepts namely IT & BPR (i.e. BE = IT + BPR).
(ii) BE is the re-thinking of business processes to improve speed, quality, & output of material or services.
(iii) The emphasis of BE is the concept of **Process Oriented Business Solutions** enhanced by the Client-server computing in IT.
(iv) The main point in BE is the efficient redesigning of company's value added chains.
(v) Value added chains are a series of connected steps running through a business which when efficiently completed add a value to enterprise & customers.
(vi) IT helps to develop business models which assists in redesigning of business processes.

26. Write short notes on Business Management in the context of ERP.

ERP merges very well with common business mgt issues like BPR, TQM, mass customization, service orientation and virtual corporation etc. The basic objective of implementing an ERP program is to put in place the applications & infrastructure architecture that effectively & completely support the enterprise's business plan & business processes.

27. What is Business Modeling? How can it be used for judging the suitability of ERP package?

The approach of ERP implementation is carried out using MIS planning. First of all, a model consisting of core business processes or activities of the business is to be developed. This is the diagrammatic representation of business as a large system with interconnection of subsystems or processes that it comprises of. The planning to arrive at the process is from top down whereas the MIS implementation is done from bottom up.

Features of Business Modeling:

(i) Business Processes
(ii) Comprehensive Functionality
(iii) Designs for all types of business
(iv) Multi-National
(v) Business Engineering
(vi) Client-server architecture
(vii) Open system

The Data model consists of two elements:

1. A diagram describing various business processes & their interactions (i.e. Blueprint).
2. An underlying Data Model.

The Reference Model can be used by various companies to list their processes & data entities and if required can be subsequently modified to suit specific nature of requirements.

List of some of the entities forming a Data Model

Entity	Description
External data	Entities outside the firm that interact with it such as customers, suppliers, competitors & distributors. Also includes predictive data regarding economy & future events in external environment.
Internal Data	Data generated from the firm's TPS, internal forecasts or parameters monitored.
Personnel Data	Mostly includes profiles of employees, their skill levels, experience & past performance on various assignments.
Payroll data	Data about salaries, tax deductions, statutory forms & other deductions.
Inventory Data	Includes inventories of raw materials, goods in progress & finished goods.

Business Modeling in Practice: Most of the ERP packages available today enable flow charting business processes using standard flow chart symbols. By connecting symbols used for users, events, tasks/functions & other organizational info, complex business info can be analyzed. All ERP packages provide standard template for each of the processes so that actual processes can be compared & deviations analyzed. Business Modeling is the basis by which one can select & implement a suitable ERP package.

28. With reference to ERP package (SAP), briefly explain three modules of Enterprise Controlling. Nov 2013

W.r.t ERP packages (SAP), three modules of enterprise controlling are given as follows:

1. **EC-CS:** This component is used for financial statutory & mgt consolidation which also allows fully automated consolidation of investments even for many companies & complex investment structures.
2. **EC-PCA:** This module/component allows to work with internal transfer prices & at the same time to have the right values from company, profit centre, and enterprise perspective in parallel. Any transaction that touches an object such as customer order,plant or cost centre allocated to a profit centre will be automatically posted to EC-PCA.

It is also possible to take data directly from EC_PCA to EC_CS consolidation to prepare complete financial statutory statements & mgt reports in parallel. This provides the mgt with a consistent view of external & internal financial mgt reports.

3. **EC-EIS (Executive Info System):** EIS allows to take financial data from EC-PCA,EC-CS or any other application & combine with any external data such as market data, industry benchmarks and/or data from non-SAP applications to build a company specific comprehensive EIS.

Important Note: Please read the topic ERP Software Package (SAP) from "Study Material".

CHAPTER 8 - INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

1. Describe briefly the common features in an ideal set of IT controls OR features of IT Standards.

The common features in an ideal set of controls are as follows:

1. Every IT using org'n uses a set of controls, perhaps unconsciously, even if, the "Controls" are to let everyone have full access.
2. An ideal set of controls for a given org'n should depend on the business objectives, budget,personality, & context of that org'n.
3. The set of control objectives (as opposed to the set of controls) can & should be constant across organizations.
4. Each org'n could use the same control framework to manage their particular controls to meet those constant control objectives.

2. What are the IS Audit Standards? List the name of some IS Audit Standards.

IS Audit Standards: These standards has a unique repository of knowledge, that often forms the basis to define the commonly accepted practices. The technical competencies & skills of professionals are assessed against these practices. IS audit standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities, effectively. ***Some of the IS audit standards are:***

(i) ISO 27001	(iv) COSO	(vii) Systrust / Webtrust
(ii) CMM	(v) COCO	(viii) HIPAA
(iii) COBIT 5	(vi) ITIL	(ix) SA 402 (Revised)

3. Which Standards on Auditing issued by ICAI are used for info system auditing & practices?

Standard on Auditing issued by ICAI:

1. **SA 315**: Identifying and assessing the risk of material misstatement through understanding the entity and its environment
2. **SA 330**: The auditors response to assessed risk

4. Write short notes on ISO 27001 - Info Security Management Standard.

ISO 27001 - Information Security Management Standard:

- ✓ ISO 27001 is the **successor of BS7799-2**;
- ✓ It is the international best practice and standard for an Information Security Management System (ISMS);
- ✓ It is a Standard written by world's best experts in the field of info security;
- ✓ The Standard was ***published jointly by*** the **International Security Office** (ISO) **and** the **International Electrotechnical Commission** (IEC);
- ✓ An ISMS is a systematic approach to managing confidential or sensitive information so that it remains secure;
- ✓ It helps an organisation to coordinate all the security efforts - both electronic & physical;
- ✓ It aims to provide a methodology for the implementation of info security in an organisation;
- ✓ It also enables an organisation to get certified, which means that an independent certification body has confirmed that info security has been implemented in the best possible way in the organisation.

5. What are the various Phases of ISMS? Explain the major activities of the first phase of ISMS. RTP Nov 2013

Four phases of ISMS:

ISO 27001 prescribes 'how to manage information security through a system of information security management'. Such a mgt system consists of four phases that should be continuously implemented in order to minimize risk to the info system.

These phases are given as follows:

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 Plan phase consists of the following steps:*** - Determining the scope of the ISMS - Writing an ISMS Policy - Risk assessment - Identification of assets, vulnerabilities and threats - Evaluating the size of risks - Identification and assessment of risk treatment options - Selection of controls for risk treatment - Obtaining management approval for residual risks - Obtaining mgt approval for implementation of the ISMS - Writing a Statement of applicability	**Do Phase [RTP May 2014]** – This phase includes carrying out everything that was planned during the previous phase ***This phase consists of the following activities:*** - Writing a risk treatment plan – describes who, how, when and with what budget applicable controls should be implemented - Implementing the risk treatment plan - Implementing applicable security controls - Determining how to measure the effectiveness of controls - Carrying out awareness programs and training of employees - Management of the normal operation of the ISMS - Management of ISMS resources - Implementation of procedures for detecting and managing security incidents.
Check Phase – The purpose of this phase is to monitor the functioning of the ISMS and check whether the results meet the set objectives ***This phase includes the following:*** - Implementation of procedures for monitoring and reviewing the security activities; - Regular reviews of the effectiveness of the ISMS; - Measuring the effectiveness of controls; - Reviewing risk assessment at regular intervals; - Internal audits at planned intervals; - Management reviews over ISMS; - Keeping records of activities and incidents relating to ISMS.	**Act Phase** – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase. ***This phase includes the following:*** - Implementation of identified improvements in the ISMS - Taking corrective and preventive action - Communicating activities and improvements to all stakeholders - Ensuring that improvements achieve the desired objectives.

6. Explain the Areas of focus of ISMS.

(i) Security Policy : [Covered in Chapter 9]

(ii) Organisational Security:

Briefly explain the 'Organisational Security with Controls & Objectives' w.r.t info security policy.

A management framework needs to be established to initiate, implement and control information security within the organization. This needs proper procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization.

The detailed control and objectives are as follows :

- **Information System Infrastructure:** To manage information security within the organisation.
- **Security of third party access:** To maintain the security of organisational information processing facilities and information assets accessed by third parties.
- **Outsourcing:** To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

(iii) Asset Classification and Control :

Briefly explain Asset Classification and Control under Info security mgt systems (ISMS). June 2009, May 2013

One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, which is appropriate for copy, store, transmit or destruction of the info asset.

An Information Asset Register **(IAR)** ***should be created*** detailing every information asset within the organisation. ***For example***:

(a) Databases (e) Test samples
(b) Personnel records (f) Contracts
(c) Scale models (g) Software licenses
(d) Prototypes (h) Publicity material

The Information Asset Register (IAR) should also describe who is responsible for each information asset and whether there is any special requirement for confidentiality, integrity or availability. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses.

The detailed control and objectives thereof are as follows:

- **Accountability for Assets :** To maintain appropriate protection of organisational assets
- **Information Classification :** To ensure that information assets receive an appropriate level of protection

Explain the 'Asset classification and security classification' in the context of an IS Security Policy. [Topic of chapter 9]

1) An inventory of assets must be maintained. This must include physical, s/w & info assets.
2) A formal, documented classification scheme should be in place and all staff must comply with it.
3) The originator or 'owner' of an item of information should provide a security classification, where appropriate.
4) The handling of information, which is protectively marked ***CONFIDENTIAL*** must be specifically approved.
5) Exchanges of data and software between organizations must be controlled. Organizations to whom information is to be sent must be informed of the protective marking associated with that information.
6) Appropriate procedures for information labeling and handling must be agreed and put into practice.
7) Classified waste must be disposed of appropriately and securely.

(iv) Personnel Security :

Briefly explain the 'Personnel Security with Controls & Objectives' w.r.t info security policy.

Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training. Alert and well-trained employees who are aware of what to look for can prevent future security breaches.

Appropriate personnel security ensures that :

- Employment contracts and staff handbooks have agreed, clear wording
- Ancillary workers, temporary staff, contractors and third parties are covered
- Anyone else with legitimate access to business information or systems is covered.

Staff training is an important feature of personnel security to ensure the Information Security Management System (ISMS) continues to be effective. Periodically, refreshers on less frequently used parts of the Information Security Management System (ISMS),such as its role in disaster recovery plans,can make a major difference when there is a need to put the theory into practice. Disaster management is a team effort and not the responsibility of a single department or person.

The detailed control and objectives thereof are as follows:

- **Security in Job definition and Resourcing :** To reduce the risks of human error, theft, fraud, or misuse of facilities .
- **User Training:** To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in course of their normal work
- **Responding to security incidents and malfunctions:** To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents

(v) Physical and Environmental Security : [Refer page 44 for explanation]

(vi) Communications and Operations Management :

Briefly explain the 'Communications & Operations mgt with Controls & Objectives' w.r.t info security policy.

Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident response procedures.Special controls should be established to safeguard

the confidentiality and integrity of data passing over public networks. Special controls may also be required to maintain the availability of the network services.
Exchange of information and software between external organizations should be controlled, and should be compliant with any relevant legislation. There should be proper information and software exchange agreements, the media in transit need to be secure and should not be vulnerable to unauthorized access, misuse or corruption.
Electronic commerce involves electronic data interchange, e-mail and online transactions across public networks such as Internet.
The detailed control and objectives thereof are as follows :

- **Operational procedures and responsibilities:** To ensure correct and secure operation of information pro cessing facility
- **System planning and acceptance:** To minimise risks of system failure
- **Protection against malicious software:** To protect the integrity of software and info
- **Housekeeping:** To maintain the integrity and availability of information processing and communication services
- **Network Management:** To ensure the safeguarding of info in networks and the protection of the supporting infrastructure
- **Media handling and security:** Prevent damage to assets and interruptions to business activity
- **Exchanges of information and software:** To prevent loss, modification or misuse of info exchanged between organizations

(vii) Access Control:

Briefly explain the 'Access Control Policy with Controls & Objectives' w.r.t info security policy.

Access to information and business processes should be controlled on the business and security requirements. This will include defining access control policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication. node authentication, segregation of networks, network connection control, network routing control. operating system access control, user identification and authentication, use of system utilities, application access control, monitoring system access and use and ensuring information security when using mobile computing and tele-working facilities.
The detailed control and objectives thereof are as follows:

- **Business requirement for access control :** To control access to information
- **User access management :** To prevent unauthorised access to info systems
- **User responsibilities :** To prevent unauthorised user access
- **Network access control :** Protection of networked services
- **Operating system access control :** To prevent unauthorised computer access
- **Application Access Control:** To prevent unauthorised access to information held in information systems
- **Monitoring System Access and use :** To detect unauthorised activities
- **Mobile Computing and teleworking:** To ensure info security when using mobile computing & teleworking facilities.

What are the major points that are needed to be taken into consideration for Access Control w.r.t IS Policy?
[Topic of chapter 9] RTP May 2013

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

(viii) Systems Development and Maintenance:

Briefly explain the 'Systems Development & maintenance with Controls & Objectives' w.r.t IS Policy. RTP May 2013

Security should ideally be built at the time of inception of a system. Hence security requirements should be identified and agreed prior to the development of information systems. This begins with security requirements analysis and specification and providing controls at every stage i.e. data input, data processing, data storage and retrieval and data output. It may be necessary to build applications with cryptographic controls. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, protection of cryptographic keys and standards to be used for cryptography. A strict change control procedure should be in place to facilitate tracking of changes. Any changes to operating system changes, software packages should be strictly controlled. Special precaution must be taken to ensure that no covert channels, back doors or Trojans are left in the application system for later exploitation.
The detailed control and objectives thereof are as follows:

- **Security requirements of system:** To ensure that security is built into information systems
- **Security in application systems:** To prevent loss, modification or misuse of user data in application system
- **Cryptographic Controls:** To protect the confidentiality, authenticity or integrity of information

- **Security of system files:** To ensure that IT projects and support activities are conducted in a secure manner
- **Security in development and support process:** To maintain the security of application system software and information

(ix) Business Continuity Management: [covered in chapter 6]

(x) Compliance:

Briefly explain the "Compliance" as the area of focus of ISMS with relevant Controls & Objectives.

It is essential that strict adherence is observed to the provision of national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and collection of evidence. Information Technology's use in business has also resulted in enacting of laws that enforce responsibility of compliance. All legal requirements must be complied with to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

The detailed control and objectives thereof are as follows:

- **Compliance with legal requirements:** To avoid breaches of any criminal and civil law, and statutory, regulatory, or contractual obligations, and of any security requirements
- **Review of security policy and technical compliance:** To ensure compliance of systems with organisational security policies and standards
- **System Audit Consideration:** To maximize the effectiveness, & to minimise interference to / from the system audit process.

7. Write short notes on 'Capability Maturity Model'. May 2011

Capability Maturity Model (CMM): CMM was ***developed by*** software engineering institute ***(SEI) of US***. It was ***designed to guide s/w organizations*** in selecting process improvement strategies. It is a model of process maturity for s/w development. It presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM is ***based on*** knowledge acquired from software process assessments and extensive feedback from both industry and government.

The development & application of CMM **helps to solve the problem of** over-running of schedule & budget in completing the projects. **The key concept** of the standard is organisational maturity. A mature organisation clearly defines the procedures for s/w development & project mgt. These procedures are adjusted & perfected as required.

8.How will you define a S/W process? What do you mean by its capability,performance & maturity? Nov 10, RTP May 13

Software Process: It is a set of activities, methods and practices that people uses to develop software. As an organization matures, the software process becomes better defined and more consistently implemented throughout the organization.

1) **Software process capabilities:** It describes the range of expected results that can be achieved by following a software process.

2) **Software process performance:** It represents the actual results achieved by following a software process.

3) **Software process maturity:** It is the extent to which a specific process is clearly defined, managed, measured, controlled & effective. ***Maturity implies a potential for growth in capability*** and indicates both ***the richness of an organisation's s/w process*** **and** ***the consistency*** ***with which it is applied in projects throughout the organisation.*** As a s/w organisation gains in s/w process maturity, it establishes its s/w process via policies, standards, and organisational structures.

9. What do you understand by 'Software Process Maturity'? Discuss five levels of Software Process Maturity of Capability Maturity Model (CMM). Practice Manual, May 2012

Software Process: It is a set of activities, methods, practices, & transformations that are used to develop & maintain s/w & the associated products, such as ***project plans, design documents, code, test cases, and user manuals.***

Software Process Maturity: It is the extent to which a specific process is clearly defined, managed, measured, controlled & effective. ***Maturity implies a potential for growth in capability*** and indicates both ***the richness of an organisation's s/w process*** **and** ***the consistency*** ***with which it is applied in projects throughout the organisation.*** As a s/w organisation gains in s/w process maturity, it establishes its s/w process via policies, standards, and organisational structures.

Five Levels of Software Process Maturity: Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organising these evolutionary steps into **5 maturity levels** that lay successive foundations for continuous process improvement. These five maturity levels are discussed below:

(i) Level 1 - The Initial Level: ***At the Initial Level***, the organization typically does not provide a stable environment for developing and maintaining software. ***Success depends*** entirely ***on*** having an exceptional ***manager*** **and** a seasoned and effective ***software team***. Success in Level 1 organizations depends on the competence and heroics of the people in the organization and cannot be repeated unless the same competent individuals are assigned to the next project. Thus, at Level 1, capability is a characteristic of the individuals, not of the organization.

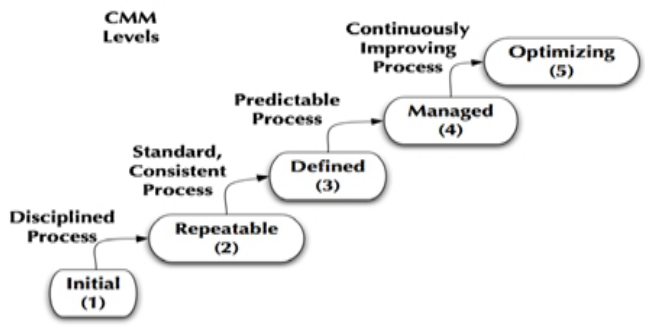


Fig. Levels of CMM

(ii) Level 2 - The Repeatable Level:

Write short notes on Level 2 - 'The Repeatable Level' of CMM. RTP May 2014

At this level, ***policies for managing a software project*** **and** ***procedures*** ***to implement those policies are established***. Planning and managing new projects is based on experience with similar projects. Projects in Level 2 organizations have installed basic software management controls. Realistic project commitments are ***based on the results observed on previous projects and on the requirements of the current project***. The software managers for a project track software costs, schedules, and functionality;

problems in meeting commitments are identified when they arise. ***The software process capability of Level 2 organizations can be summarized as*** **disciplined** because planning and tracking of the software project is stable and earlier successes can be repeated. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.

(iii) Level 3 - The Defined Level: ***At this level***, the standard process for developing and maintaining software across the organization is documented, including both software engineering and management processes, and these ***processes are integrated into a coherent whole***. This standard process is ***referred to*** throughout the CMM ***as the organization's standard software process***. Processes established at Level 3 are ***used to help the software managers and technical staff*** perform more effectively. The organization exploits effective software engineering practices when standardizing its software processes. There is a group who is responsible for the organisation's s/w process activities, ***e.g.*** **Software engineering process group (SEPG)**. ***An organisation-wide training program is implemented*** to ensure that the staff & managers have required skills & knowledge to fulfil their assigned roles.

The software process capability of Level 3 organizations can be summarized as **standard and consistent** because both software engineering and management activities are stable and repeatable. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process.

(iv) Level 4 - The Managed Level: ***At this level***, the ***organization sets quantitative quality goals for both software products and processes.*** Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. ***An organization-wide software process database is used*** to collect and analyze the data available from the projects' defined software processes. Software processes are instrumented with well-defined and consistent measurements at Level 4.

The software process capability of level 4 organizations can be summarized as being **quantifiable and predictable** because the process is measured and operates within measurable limits. This level of process capability allows an organization to predict trends in process and product quality within the quantitative bounds of these limits. Because the process is both stable and measured, when some exceptional circumstance occurs, the "special cause" of the variation can be identified and addressed. When the known limits of the process are exceeded, action is taken to correct the situation. Software products are of predictably high quality.

(v) Level 5 - The Optimizing Level: ***At this level***, the entire ***organization is focused on*** **'continuous process improvement'**. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Software project teams in Level 5 organizations analyze defects to determine their causes. Software processes are evaluated to prevent known types of defects from recurring, and lessons learned are disseminated to other projects.

The software process capability of Level 5 organizations can be characterized as **'continuously improving'** because Level 5 organizations are continuously striving to improve the range of their process capability, thereby improving the process performance of their projects. ***Improvement occurs*** **both by** ***incremental advancements*** in the existing process **and by** ***innovations*** using new technologies and methods. Technology and process improvements are planned and managed as ordinary business activities.

10. Write short notes on COBIT 5 - IT Governance Model.

COBIT stands for 'Control objectives for info & related technology. It is an IT governance framework & supporting toolset that allows managers to bridge gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout the organizations. It emphasizes regulatory compliance & helps organizations to increase the value attained from IT.

- ***COBIT 5 is the latest edition of*** "Information System Audit and Control Association" (**ISACA**) ***released in April 2012***.
- **It builds & expands on** ***COBIT 4.1*** ***by integrating*** other major frameworks, standards & resources, including ISACA's ***Val IT & risk IT***, Info Technology Infrastructure Library (***ITIL***) **and** related standards from the International Organisation for Standardization (***ISO***).
- It reflects the central role of info & technology in creating value for enterprises. It provides globally accepted principles, practices, analytical tools & models to help increase the trust in, value from info system. These principles, practices, analytical tools & models represent leadership & guidance from business, IT & governance experts around the world.

11. Why is there Need for enterprises to use COBIT 5? What are the benefits derived from it?

Need for Enterprises to use COBIT 5: Enterprises depend on good, reliable, repeatable data, on which, they can base good business decisions. COBIT 5 provides practices in governance & mgt to address these critical business issues. It helps enterprises create optimal value from their info & technology. COBIT 5 provides the tools necessary to understand, utilize, implement & direct important IT related activities, and make more informed decisions through its use. COBIT 5 is intended for enterprises of all types & sizes, including non-profit & public sector and is designed to deliver business benefits to enterprises, including:

1. Increased value creation from use of IT; user satisfaction with IT engagement & services; reduced IT-related risks & compliance with laws, regulations & contractual requirements.
2. The development of more business-focused IT solutions & services.
3. Increased enterprise wide involvement in IT-related activities.

Benefits of COBIT 5: It helps enterprises of all sizes to -

- maintain high-quality information to support business decisions
- achieve strategic goals and realize business benefits through the effective use of IT
- achieve operational excellence through reliable, efficient application of technology
- maintain IT-related risk at an acceptable level
- optimize the cost of IT services and technology
- support compliance with relevant laws, regulations, contractual agreements and policies.

- **Customizing COBIT as per the need:** COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Because of its open design, ***it can be applied to meet needs related to:***

(i) Information security
(ii) Risk management
(iii) Governance and management of enterprise IT
(iv) Assurance activities
(v) Legislative and regulatory compliance
(vi) Financial processing or CSR reporting

12. Explain how COBIT 5 integrates with other frameworks.

COBIT 5 is a comprehensive framework and is based on overall enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance. It also provides a basis to integrate effectively other frameworks, standards & practices used, such as -

(i) ITIL
(ii) TOGAF (The Open Group Architecture Framework)
(iii) ISO 27000
(iv) GEIT (Governance of Enterprise IT) standard ISO/IEC 38500:2008

Thus COBIT 5 acts as the single primary framework which serves as a consistent and integrated source of guidance in a non-technical common language. ***The framework can be aligned with:***

- Enterprise policies, strategies, governance and business plans, and audit approaches
- Enterprise risk management framework
- Existing enterprise governance organisation, structures and processes

13. Explain the Five Principles of COBIT 5 in detail. **RTP May 2014**

COBIT 5 simplifies governance challenges with just 5 principles & 7 enablers. The five key principles for governance & mgt of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance & mgt framework that optimises info & technology investment and use for the benefit of stakeholders.

Principle 1: Meeting Stakeholders Needs - COBIT 5 provides all of the required processes & other enablers to support business value creation through the use of IT. Because, every enterprise has different objectives, an enterprise can customise COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT-related goal & mapping these to specific processes & practices.

Fig. Principles of COBIT 5

Principle 2: Covering the Enterprise End-to-End -

- COBIT 5 covers all functions & processes within the enterprise and treats info & related technologies as assets.
- It considers all IT related governance & mgt enablers to be enterprise-wide & end-to-end, i.e., inclusive of everything and everyone (internal & external) that is relevant to governance & mgt of enterprise info and related IT.

Principle 3: Applying a Single Integrated Framework

- There are many IT-related standards and best practices, each providing guidance on a subset of IT activities;
- COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, and thus, allows the enterprise to use COBIT 5 as the primary governance and management framework integrator.

Principle 4: Enabling a Holistic Approach

- Efficient and effective governance & management of enterprise IT require a holistic approach, taking into account several interacting components;
- COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance & management system for enterprise IT.Enablers are broadly defined as anything that can help achieve the objectives of the enterprise.

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 organisational structures and serve different purposes

- **Governance:** In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises
- **Management:** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer.

14. Describe Various Categories of Enablers under COBIT 5. **RTP Nov 2013**

COBIT 5 Enablers: Enablers are factors that, individually and collectively, influence whether something will work— in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve. ***The COBIT 5 framework describes seven categories of enablers*:**

1. **Principles, policies and frameworks:** These are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
2. **Processes:** They 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.
3. **Organizational structures:** These are the key decision-making entities in an enterprise.
4. **Culture, ethics and behavior** of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
5. **Information:** It is widespread throughout any organization and includes all information produced and used by the enterprise.

6. **Services, infrastructure and applications:** They include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
7. **People, skills and competencies:** These are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

15. Write short notes on COBIT 5 Process Reference Model.

- ✓ This model defines & describes in detail a no. of governance & mgt processes.
- ✓ It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT & business managers.
- ✓ Each enterprise must define its own process set, taking into a/c its specific situation.
- ✓ It also provides a framework for measuring & monitoring IT performance, providing IT assurance, communicating with service providers, and integrating best mgt practices.

16. Write short notes on CoCo Model. Imp.

CoCo stands for **"Criteria of Control".** It was ***published in 1995 by*** the Canadian Institute of Chartered Accountants (**CICA**). It builds on COSO and can be said as a concise superset of COSO **i.e "Committee of sponsoring organizations"**. CoCo is a ***'guidance"*** and it is ***"useful in making judgments"*** about **"designing, assessing & reporting on the control systems of organizations."** In this way, CoCo can be seen as a model of controls for info assurance, **rather than** a set of controls.

17. CoCo Model identifies three objectives, What are they?

CoCo model identifies three objectives:

1. Effectiveness and efficiency of operations
2. Reliability of internal and external reporting, and
3. Compliance with applicable laws and regulations and internal policies

18. List the four Interrelated Elements of Internal Control recognised by CoCo Model.

CoCo model recognizes four interrelated elements of internal control:

1. **Purpose** – i.e an organisation that performs a task is guided by an understanding of the purpose of the task.
2. **Capability** – i.e supported by capabilities like information, resources, supplies and skill.
3. **Commitment** – i.e to perform the task well over the time, the organization needs a sense of commitment.
4. **Monitoring and learning** – i.e the organization must monitor task performance to improve the task process.

19. Explain the four important Concepts about "Control" given under CoCo Model.

Four important concepts about "control" as per CoCo are as follows:

1. Control is affected by people throughout the organization, including the **B.O.D** (or its equivalent), mgt & all other staff.
2. People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of control that supports achievement of those objectives
3. Organizations are constantly interacting and adapting.
4. Control can be expected to provide only reasonable assurance, not absolute assurance.

20. What is IT Infrastructure Library?

- ➢ ITIL ia an acronym used for **"Information Technology Infrastructure library".**
- ➢ It was originally created by UK Government and thereafter it was rapidly adopted across the world for IT services.
- ➢ It is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business.
- ➢ It is published in a series of **5 core publications**, each of which covers an ITSM life cycle stage.
- ➢ It describes procedures, tasks and checklists, used by any organization for establishing a minimum level of competency in its IT services.
- ➢ Based on a core of 5 titles, the changes in ITIL V3 reflect the way ITSM has matured over the past decades and change the relationship b/w IT & business.
- ➢ ITIL V3 integrates into a single life cycle whereas, previously ITIL worked to align service mgt with business strategy.

21. Explain the ITIL framework, in detail. OR Explain the 5 Volumes of ITIL in detail.

The details of 5 volumes of ITIL are as follows:

1. Service Strategy: Strategy deals with the strategic management approach in respect of ITSM. **It provides guidance on:**

- ➢ **Leveraging service management capabilities -** to effectively deliver value to customers and illustrate value for service providers;
- ➢ **The design, development, and implementation of service management;**
- ➢ **The principles underpinning the practice of service mgt** to aid the development of service mgt policies, guidelines, and processes across the ITIL life cycle.

However, Service strategy have far-reaching consequences including those related to delayed effect.

2. Service Design: It 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. **The Service Design volume provides guidance on:**

- ➢ **Design & development of services;** and
- ➢ **Service mgt processes**.

It includes design principles & methods for converting strategic objectives into portfolios of services and service assets. Service design is not limited to new services but it includes the changes & improvements required to maintain or increase the value to customers over the life cycle of services.

3. Service Transition: The Service Transition volume provides guidance on:

- **Development & improvement of capabilities -** for switching new & changed services into operations. Guidance is provided on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation, whilst controlling the risks of failure and disruption;
- **Managing the complexity of changes to services and service management processes -** to prevent undesired consequences whilst permitting for innovation;
- **Transferring the control of services between customers and service providers;**
- **Service design & implementation**, ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively.

4. Service Operation:

Write short notes on 'Service Operation' under ITIL V3. RTP May 2014

It provides detailed guidelines on processes, methods, and tools in addressing the proactive and reactive control perspectives. Managers & practitioners are provided with ***knowledge***; enabling them to make better informed decisions ***in the areas*** such as ***managing the availability of services***, ***controlling demand***, ***optimizing capacity utilization***, ***scheduling of operations***, and ***fixing problems***. ***It provides guidance on:***

- The day-to-day management of IT service;
- Supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce;
- Techniques to maintain service operations stability and at the same time allowing for changes in design, scope, scale, and service levels.

5. Continual Service Improvement: It combines principles, practices, and methods from change management, quality management, and capability improvement to achieve incremental and significant improvements in service quality, operational efficiency, and business continuity. **It provides guidance on:**

(i) **The measurement of service performance through the service life-cycle**, suggesting improvements to ensure that a service delivers the maximum benefit

(ii) **Creating and Maintaining value for customers** through improved design, introduction, and operation of services

(iii) **Linking improvement efforts and outcomes** with service strategy, design, and transition, focusing on increasing the efficiency, maximizing the effectiveness and optimizing the cost of services and the underlying ITSM processes.

21. Write short notes on SysTrust and WebTrust services. Nov 2010

SysTrust and WebTrust: These are two specific services **developed by the AICPA** that are based on the Trust Services Principles and Criteria. ***SysTrust engagements are designed for*** the provision or advisory services or assurance on the reliability of a system. ***WebTrust engagements relate to*** assurance or advisory services on an organization's system related to e-commerce.

Only certified public accountants (CPAs) may provide the assurance and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.

The following principles & related criteria have been developed by the AICPA for use by practitioners in the performance of trust services engagements such as SysTrust & WebTrust.

1. Security: The system is protected against unauthorized access(both physical and logical).

2. Availability: The system is available for operation and use as committed or agreed.

3. Processing integrity: System processing is complete, accurate, timely, and authorized.

4. Online privacy: Personal info obtained as a result of e-commerce is collected, used, disclosed & retained as committed or agreed.

5. Confidentiality: Information designated as confidential is protected as committed or agreed.

22. Explain the Areas under which the principles & criteria of SysTrust & WebTrust services are organised.

Each of the Principles and Criteria of SysTrust & WebTrust services are organized and presented in four broad areas:

1. Policies: The entity has defined and documented its policies relevant to the particular principle.

2. Communications: The entity has communicated its defined policies to authorized users.

3. Procedures: The entity uses procedures to achieve its objectives in accordance with its defined policies.

4. Monitoring: The entity monitors the system and takes action to maintain compliance with its defined policies.

At the completion of a SysTrust engagement, the practitioner renders an opinion on the management's assertion that effective controls have been maintained. The practitioner can report on all the SysTrust & WebTrust principles together or on each separately.

23. Write short notes on HIPAA. Nov 2011

HIPAA stands for **"The Health Insurance Portability and Accountability Act"** was enacted by the U.S. Congress in 1996. It has two main segments:

- **Title I of HIPAA** protects health insurance coverage for workers and their families when they change or lose their jobs.
- **Title II of HIPAA**, known as the Administrative Simplification (AS) provisions, requires the establishment of National Standards for electronic health care transactions & National Identifiers for health service providers, health insurance plans, & employers.

24. Explain the Security Rule issued under HIPAA. Also explain the types of security safeguards required for compliance.

The Security Rule: The Final Rule on Security Standards was issued on ***Feb 20, 2003***. It took effect on ***April 21, 2003*** with a compliance date of ***April 21, 2005*** for most covered entities and ***April 21, 2006*** for "small plans".

The Security lays out ***three types of security safeguards for compliance***, which are ***Administrative, Physical, and Technical.*** For each of these types, the Rule identifies various security standards, and for each standard, it names both required & addressable implementation specifications.

- **Required Specifications:** These must be adopted & administered as dictated by the Rule.
- **Addressable Specifications:** These are more flexible. *Individual covered entities** can evaluate their own situation & determine the best way to implement addressable specifications.

*** *Covered entities* -** i.e the entities that must comply with HIPAA requirements.

***The Standards and Specifications are as follows*:**

1. Administrative Safeguards:

Write short notes on 'Administrative Safeguards' under HIPAA Security Rule.

Policies & procedures should be so designed that it should clearly show how the entity will comply with the act. It covers:

- ❖ The covered entities must adopt a written set of privacy procedures, and designate a privacy officer who should be responsible for developing & implementing all required policies & procedures;
- ❖ Procedures must address access authorization, establishment, modification, and termination;
- ❖ Procedures should clearly identify employees or classes of employees who will have access to protected health info (PHI). Access to PHI in all forms must be restricted to only those employees who have a need for it to complete their job function;
- ❖ Entities must show that an appropriate ongoing training program regarding the handling PHI is provided to employees;
- ❖ Covered entities that outsource some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements;
- ❖ A Contingency plan should be in place for responding to emergencies.

2. Physical Safeguards:

Write short notes on 'Physical Safeguards' under HIPAA Security Rule.

Controlling physical access to protect against inappropriate access to protected data. It covers:

- Controls must govern the **introduction & removal of h/w & s/w** from the network***;***
- **Access to equipment containing health info** should be carefully controlled & monitored;
- **Access to h/w & s/w must be limited** to properly authorized individuals;
- **Policies** are required to address proper workstation use;
- If the covered entities utilize **contractors or agents**, they **must be fully trained** on their physical access responsibilities.

3. Technical Safeguards:

Write short notes on 'Technical Safeguards' under HIPAA Security Rule.

Controlling access to computer systems and enabling covered entities to protect communications containing protected Health Info (PHI) transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.It covers-

- ◆ Info system housing PHI must be protected from intrusion;
- ◆ Each covered entity is responsible for ensuring that the data within its system has not been changed or erased in an unauthorized manner;
- ◆ Covered entities must also authenticate the entities with whom it communicates;
- ◆ Covered entities must make documentation of their HIPAA practices available to the govt to determine its compliance;
- ◆ IT documentation should also include a written record of all configuration settings on the components of network;

25. Write short notes on SA 402 (Revised).

SA 402 (Revised) - "*Audit considerations relating to an entity using service organizations*"

- ✓ It is a revised version of the erstwhile Auditing & Assurance Standard AAS 24, issued by the ICAI.
- ✓ This Standard deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations.
- ✓ It also deals with the aspects like obtaining an understanding of the services provided by a service organization, including internal control, responding to the assessed risks of material misstatement, **Type 1 and Type 2 Reports,** fraud, non-compliance with laws & regulations, and uncorrected misstatements in relation to activities at the service organization & reporting by the user auditor.

CHAPTER 9
DRAFTING OF IS SECURITY POLICY, AUDIT POLICY, IS AUDIT REPORTING – A PRACTICAL PERSPECTIVE

What is info system security? Bring out the importance of info system security. Nov 2007

Info Systems Security: It relates to the protection of valuable IS assets against loss, disclosure, or damage. Securing valuable assets from threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is commonly understood & implemented by most organizations. Security includes both **physical security like** doors, locks, fences, insurance etc and **logical security like** user ID, password, firewalls etc.

Importance of Info System Security: The importance of IS security is widely accepted by the organizations in a global info society, where info travels through cyberspace. The security of info systems is important due to following reasons:

- The organizations depend on timely, accurate, complete, valid, consistent, relevant, & reliable info;
- Executive mgt has a responsibility to ensure that the organization provides all users with a secure info systems environment;
- There are many direct & indirect risks associated with info systems due to which there must be adequate IS security;
- The threats to info systems may compromise the CIA of info systems, that is why, the IS security is must.

Why is there need to implement Security policies in an organization? [Topic of chapter 3]

Every organization should have a security policy that defines acceptable behaviour and the reaction of the organization when such behaviour are violated. Security policies are not unique and might differ from organization to organization. Also legislation relating to Information technology is becoming more prolific, with many countries enacting laws on issues such as copyright and software privacy, intellectual property and personal data. These commercial competitive and legislative pressure require the implementation of proper security policies.

Briefly explain the 'Security Policy with Controls & Objectives' w.r.t info security policy. [Topic of chapter 8]

This activity involves a thorough of the organization business goals and its on information security. It should be implement able, easy to understand and must balance the level of protection with productivity.

The policy should cover -

- a definition of information security
- a statement of management intention supporting the goals and principles of information security
- allocation of responsibilities for every aspect of implementation
- an explanation of specific applicable proprietary and general, principles, standards and compliance requirements.
- an explanation of the process for reporting of suspected security incidents
- a defined review process for maintaining the policy document
- means for assessing the effectiveness of the policy embracing cost and technological changes
- nomination of the policy owner

The detailed control and objectives are as follows:

- **Information Security Policy:** To provide management direction and support for information security
- **Information System Infrastructure:** To manage information security within the organisation
- **Security of third access:** To maintain the security of organisational information processing facilities and information assets accessed by third parties.
- **Outsourcing:** To maintain the security of information when the responsibility for information processing has been outsourced to another organisation

What are the causes that have led to a gap b/w the need to protect systems & the degree of protection applied?

Besides there are many direct & indirect benefits derived from the use of info systems, there are also many direct & indirect risks relating to the info systems, that have led to a gap b/w the need to protect systems & the degree of protection applied. **This gap is caused by:**

- Widespread use of technology;
- Inter-connectivity of systems;
- Elimination of distance, time and space as constraints;
- Unevenness of technological changes;
- Decentralization of management control;
- Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations;
- External factors such as legislative, legal, and regulatory requirements or technological developments.

What are the reasons for 'Threats to info systems'.

Threats to information systems may arise from:

- **Technical reasons:** Program errors, bugs and crashes etc;
- **Natural disasters:** Floods, earthquake, thunderbolts etc;
- **Environmental conditions:** Power failure, brown-out, surge, pests etc;
- **Human factors:** Negligence, lack of awareness, lack of training etc;
- **Unauthorized access:** Hacking, intrusion, virus, Trojan horse, worms etc;
- **Business dependencies:** Loss of management control over outsourced activities.

What is 'Security objective'. Explain the three universally accepted attributes of security objective.

Security failures may result in both financial losses and/or intangible losses, such as unauthorized disclosure of competitive or sensitive info. Adequate measures for info security help to ensure the smooth functioning of info systems & protect the organization from loss or embarrassment caused by security failures. Therefore, the objective of information systems security is:

- The protection of interest of those relying on information;
- The protection of info systems & communications that deliver the info, from the harm resulting from the failures of CIA.

For an organization, the security objective comprises three universally accepted attributes, these are -

1. **Confidentiality:** Data and information is disclosed only to those who have the right to know it.
2. **Integrity:** Data and information is protected against unauthorized modification.
3. **Availability:** Information system is available and usable when required.

The relative priority & significance of CIA vary accordingly to the data within the IS & the business context in which it is used.

What information is sensitive?

In any organization, following types of information is generally sensitive information which needs to be protected carefully:

• **Strategic plans:** Most organizations acknowledge that strategic plans are crucial to the success of a company.But indeed, many of them fail to make efforts to protect these plans. As these plans determine the organizations competitive edge, if such information is somehow acquired by the competitors then the organization can suffer heavy financial loss as well as loss of competitive edge. **For E.g.** if marketing strategy of a new product is disclosed early to the competitors then the company may face difficulties in marketing its products effectively.

• **Business operations:** These consist of an organisation's processes & procedures, most of which are ***proprietary in nature*** and are designed by the organization after doing much R & D over them. Such processes and operations should not be disclosed to the outsiders in any case. If such information is disclosed then the company can loose its competitive edge.

E.g. A company's list of customers & vendors and the price charged for products & services is a critical info which can be damaging in the hands of a competitor. Such info is required appropriate protection, so that it should not be disclosed to someone.

• **Finances:** Financial information like salary structure of employees is ***sensitive in nature*** since if this information is disclosed to the competitors then they may be able to price their products accordingly and the company may loose its low-cost advantage.

Discuss major points, which may be considered for establishing better information protection. Nov 2012, RTP May 2014

Major points that need to be considered for establishing better information protection are as follows:

1. Not all data has the same value: Organizations must determine ***value of information*** before planning the level of protection to be provided to that information. All data and information should be classified according to its criticality and then security measures should be designed accordingly. ***For example information can be classified as follows:***

(i) Top secret (ii) Highly confidential (iii) Proprietary (iv) Internal use only (v) Public document

2. Know where the critical data resides: In today's business environment, information system is becoming more and more wide and complex. Networking has further increased the complexity of the systems environment. In such a case it is important to know exactly where the data resides so that different level of protection can be applied over it.

3. Develop an access control methodology: The organization has to develop access control mechanism to protect its data. The access control should be wide enough to cover every terminal, network and servers including application software and systems software. For important data, access controls and the related logs should extend to file level.

4. Protect information stored on media: Use of computer media like floppy disk, CD and USB drives should be controlled since any employee can use such media to copy and transfer sensitive data outside the organization. Also, when migrating from one system to another or while disposing the old systems, the status of hard drives should be checked and controlled.

5. Review hardcopy output: The hardcopy (printouts) of employees' routine work is also required to be reviewed and controlled. The final form of any strategic plan is normally protected by an organization but the rough drafts & working papers are often left unattended. Wherever necessary paper shredder should be used to destroy such hardcopy of redundant working papers.

Write short notes on basic ground rules for protecting computer-held information system. Nov 2012

A few basic ground rules that must be addressed sequentially are given as follows:

Rule #1: We need to know what the information systems are and where these are located.

Rule #2: We need to know the value of the information held and how difficult it would be to recreate if it were damaged or lost.

Rule #3: We need to know who is authorized to access the information and what they are permitted to do with the information.

Rule #4: We need to know how quickly information needs should be made available if it become unavailable for whatever reason.

Explain the types of protection that an organization can use to protect the information. Nov 2009

Explain Preventive & Restorative Info Protection with the help of examples. May 2012, RTP May 2013

I. **Preventive information protection:** In this type of protection, security controls are implemented for the protection of info against unauthorized access, modification or deletion. These controls are grouped as:

- **Physical control:** E.g. doors, locks, guards, CCTV, paper shredders, fire extinguishers
- **Logical control:** E.g. access control system, user ID's, passwords, access control list, account privileges
- **Administrative controls:** E.g. security awareness, user account maintenance and revocation, security policies.

II. **Restorative information protection:** Events that damage the information system will happen, therefore it is necessary to have an effective and timely information back-up and recovery procedure. The main requirement of any restorative information protection plan is that information lost can be recovered. This is frequently an issue that many organizations fail to properly address. If an organization can't recover or recreate critical info systems in an acceptable time period, the organization will suffer & possibly have to go out of the business.

Here are a few questions that any restorative info system protection program must address, these are -

- Has the recovery procedures been tested recently?
- How long did it take ?
- How much productivity was lost during back-up and restoration procedure?
- Did everything go according to plan?
- How much extra time was required to input the data changes since the last backup?

Write short notes on 'Holistic Protection'.

Holistic protection: Protecting corporate info systems from harm or loss is not an easy task. Protection must be done holistically (i.e which covers the whole system) and give the organisation the appropriate level of security at a cost which is acceptable to the business. IS auditor must plan for -

- Unexpected, unknown, and worst events that may happen;
- How to recover from these events if & when they occur?

However, the organizations who wait until the last minute to decide on a protection plan & recovery process ***will suffer***.

What is the Information Security Policy? What are the issues it should address? June 2009, May 2013

Meaning of Policy: A policy is a plan or course of action, designed to influence decision, actions and other matters.

Meaning of Information Security Policy: The security policy is a set of laws, rules and practices that regulates how assets including sensitive information are managed, protected and distributed within the user organization.

An information security policy addresses many issues such as disclosure, integrity and availability concern, who may access what information and in what matter, maximized sharing versus least privilege, separation of duties, who controls and who owns the information and authority issues.

Issues to address: The IS policy state senior management's commitment to information security and it must be duly signed by the appropriate senior manager. It should at least address the following issues:

(i) A definition of information security,
(ii) Reasons why information security is important to the organization, and its goal and principles,
(iii) A brief explanation of the security policies, principles, standards and compliance requirement,
(iv) Definition of all relevant information security responsibilities,
(v) Reference to supporting documentation.
(vi) IS policy must always take into a/c business requirements. **For e.g.** E-commerce security.
(vii) Policy must consistently take into account the legal, statutory, regulatory and contractual requirement.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents.

Who are the 'Members of Security Policy'.

Security policy broadly comprises the following three groups of management:

♦ **Management members** who have budget and policy authority
♦ **Technical group** who know what can and cannot be supported
♦ **Legal experts** who know the legal ramification of various policy charges

Discuss Various Types of Information Security policies and their hierarchy. Nov 2008, Nov 2011

Major info security policies are given as follows:

1. Information Security Policy: This policy provides a definition of Information security, its overall objectives and importance.

2. User security policy: This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for users, line managers, & system owners.

3. Acceptable Usage Policy: This sets out the policy for acceptable use of email and internet services.

4. Organization Information Security Policy: This policy set out group policy for the security of information assets and the information technology(IT) systems.

5. Network & system policy: This policy applies to IT deptt. users. It sets out detailed policy for system and network security.

6. Information classification policy: This policy sets out the policy for the classification of information.

7. Condition 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.

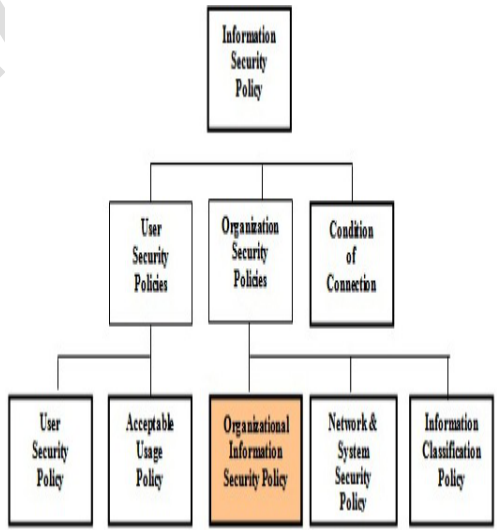


Fig. The hierarchy of Info Security Policies

What should be the major Components of a good Security Policy as per your opinion? May 2012

A good security policy should clearly state the following:

(i)Purpose and scope of the security and the intended audience
(ii) The Security infrastructure
(iii) Security policy document updation and compliance requirements
(iv) Incident response mechanism and incident reporting
(v) Security organization structure
(vi) Inventory and classification of assets
(vii) Description of technologies
(viii) Physical and environmental security
(ix) Identity Management and access control
(x) IT Operation management
(xi) IT Communications
(xii) System Development and Maintenance Controls
(xiii) Business Continuity Planning
(xiv) Legal Compliances
(xv) Monitoring and Auditing Requirements
(xvi) Underlying Technical Policy

What is the Purpose & Scope of IS Security Policy?

The primary objective of the policy would be to ensure confidentially, integrity and availability of information and related systems. **The security policy is designed to -**

a) Deny unauthorised access of any IT resources, and restrict access to data & resources or IT processes.
b) Within the operational constraints, the security control will allow the required services to be available to authorised users only.
c) The scope defines how far the policy would be applicable, to whom it would be applicable and the period for which the policy would be applicable.

Explain the Security Organization Structure.

Explain the Security responsibility and the line of reporting in an organisation, in detail.

The security responsibility and the line of reporting in the organization should be defined as below -

1) **Information security Forum (ISF):** This forum is ***chaired by*** the ***GSO*** and includes senior representative from each of the divisions within the group, together with the AGSO. It is the role of this forum to ensure that there is clear direction and visible management support of security initiative within the organization.

2) **Information Security Management Group (ISMG):** This cross functional group is ***chaired by*** the ***AGSO*** and comprises of a Divisional System Security Officer(DSSO) from each of the division, together with the IT security officer, and personnel and facilities management security officers. Its role is to co-ordinate the implementation and management of information security control across all of the division and sites.

3) **Group security officer (GSO):**The GSO will have overall responsibility for security within the group. This includes the security of all information assets, the network accreditation scheme and non-IT security.

4) **Assistant Group Security Officer (AGSO):** The AGSO ***reports to*** the ***GSO*** and the information security forum and is responsible for the coordination of information security implementation and management across the group.

5) **IT Management:** IT management have overall responsibility for security of the IT infrastructure. This is discharged mainly through installation security officers and the it security officer.

6) **IT Security Officer (ITSO):** The ITSO ***reports to*** the ***ISMG***. The ITSO is responsible for managing IT security programmes and IT security incidents.

7) **Installation Security Officer (ISO):** An ISO will be appointed for each IT environment from the IT team leaders. ISO will be responsible for all security matters related to their system/installation and network.

8) **Personnel Security Officer (PSO):** The PSO will ***report*** directly ***to personnel management*** on all security matters relating to personnel. The role involves ensuring the controls set out are implemented, adhered to and reviewed as necessary.

9) **Facilities Management Security Officer (FMSO):** The FMSO will ***report*** directly ***to facilities management*** on all security matters relating to personnel. The role involves ensuring the controls are implemented,adhered to and reviewed as necessary.

10) **Divisional System Security Officer (DSSO):** SSO from each division will be appointed as a DSSO. The DSSO carries the same responsibilities as a SSO and in addition is responsible for representing the SSO in their division at the ISMG.

11) **System Security Officer (SSO):** A senior user will be appointed to fulfill the role of system security officer for each major application system or group of systems. SSO responsibilities focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.

12) **System Owner:** System owners carry the overall responsibility for the information security of their own systems. They are responsible for allocation of protective marking to their systems and data according to the information classification policy and all staff for treating protectively marked material accordingly.

13) **Line Managers:** All line managers are responsible to take appropriate steps to ensure that all live or developing IT systems compliance with the aims and objectives of this policy.

14) **Users:** All users of live IT systems are required to comply with the security procedures for their system and any applicable general IT security guidance.

Write short notes on 'Responsibility Allocation' in an IS Security Policy.

Responsibility Allocation: The responsibilities of management and information security should be set out in the policy and includes as follows -

1) An owner Would be appointed for each information asset.
2) All staff should be aware of the need for information security and their responsibilities.
3) All the tasks have been completed successfully & the system owner is satisfied.
4) All new network communication links must be approved.
5) A contact list of organizations that may be required in the event of a security incident to be maintained.
6) Risk assessments for all third party access to the information assets must be carried out.
7) Access by third parties to all material must be strictly limited and controlled.
8) All outsourcing contract must detail all major changes to software and hardware.

'Asset classification & Security classification' - Refer chapter 8

'Access Control' - Refer chapter 8

Write short notes on 'Incident Handling'.

For incident handling, following are the major points:

(i) Security incident reporting time and approach must be consistent at all times. Specific procedures must be introduced to ensure that incidents are recorded and any recurrence is analyzed to identify weaknesses or trends.

(ii) Procedures for the collection of evidence relating to security incidents should be standardized. All staff must be made aware of the process. Adequate records must be maintained and should be inspected to enable the investigation of security breaches or intensive attempts by third parties to identify security weaknesses.

'Business continuity management' - Refer chapter 6

Write short notes on 'System Development and Maintenance Controls'.

■ System development or enhancement must have appropriate security controls included to safeguard their availability and ensure confidentiality of the information they process.

■ All security requirements and controls must be identified and agreed prior to the development of information systems

Write short notes on the Purpose of Audit Policy. **June 2009, May 2013**

The Purpose of audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. The Audit is done to protect entire system from the most common security threats such as access to confidential data, unauthorized access of the department computers, password disclosure compromise,virus infections,denial of service attacks etc. Audits may be conducted to ensure integrity, confidentiality and availability of information and resources. The IS Audit Policy should lay out the objective and the scope of the audit. **An IS audit is conducted to:**

(i) safeguard the Information System Assets/Resources,
(ii) maintain the Data Integrity,
(iii) maintain the System Effectiveness,
(iv) ensure System Efficiency, and
(v) comply with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

Write some common security threats from which an info system may be protected through IS Audit.

The IS audit is done to protect entire system from the most common security threats which includes the following:

(i) Access to confidential data
(ii) Unauthorised access to the department computers.
(iii) Password disclosure compromise
(iv) Virus infections
(v) Denial of service attacks
(vi) Open ports, which may be accessed from outsiders
(vii) Unrestricted modems unnecessary open ports.

What is the scope of IS Audit? Explain the categories of IS Audit. **June 2009, Nov 2012**

The scope of IS Audit process should include the examination & evaluation of adequacy & effectiveness of system of internal controls and the quality of performance by info system. In addition, IS audit will also examine & evaluate the planning, organizing & directing processes to determine whether reasonable assurance exists so that the objectives & goals will be achieved. Such evaluations, in the aggregate provide info to appraise the overall system of internal controls.

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

Categories of IS Audits:

IS audits has been categorized into following five major types types:

(i) Systems and Applications: To ensure valid, reliable, timely, & secure input, processing, & output at all levels of a system's activity.

(ii) Information Processing Facilities: To ensure timely accurate, and efficient processing.

(iii) Systems Development: To ensure 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.

(iv) Management of IT and Enterprise Architecture: To verify 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: To verify that controls are in place on the client, server, and on the network connecting client and server.

Explain the areas to be examined by an IS auditor under IS audit.

The IS auditor will examine the followings -

- Information system mission statement and agreed goals and objectives.
- Assessment of the risks associated with the use of the information systems and approach to managing those risks.
- Information system strategy plans to implement the strategy and monitoring of progress.
- Information system budgets and monitoring or variances.
- Policies for information system use and monitoring of compliance with these policies.
- Major contract approval and monitoring of performance of the supplier.
- Monitoring of performance against service level agreement.
- Acquisition of major systems and decisions on implementation.
- Impact of external influence on information system such as internet.
- Control of internal and external audit reports, quality assurance reports or other reports on information system.
- Business Continuity Planning, and Testing.
- Compliance with legal and regulatory requirements.

As an IS Auditor, what are the steps to be followed by you while conducting Information Technology Auditing? **May 2012**

IT auditing can be categorized into six stages-

(i) Scoping and Pre-Audit Survey: In this stage the auditors determine the main areas of focus based on some risk-based assessment. Information sources at this stage include background reading, previous audit reports, pre-audit interview, observations etc.

(ii) Planning and preparation: In this stage scope is converted into plan including risk-control-matrix.

(iii) Fieldwork: In this stage the actual audit work is performed by gathering evidence by interviewing staff and managers, reviewing documents, observing processes etc.

(iv) Analysis: In this stage,the auditor sort & review all the evidence gathered earlier. SWOT/ PEST techniques can be used for analysis.

(v) Reporting: In this stage reporting to the management is done after analysis.

(vi) Closure: In this stage preparing notes for future audits and following-ups done. Steps 3 and 4 may on occasions involve the use of automated data analysis tools such as ACL or IDEA, Excel, Access and SQL queries.

What are the aspects covered in IS Audit Process?

The focus of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness and efficiency. The Audit of an IS environment may include one or both of the following:

♦ Assessment of internal controls.
♦ Assessment of the efficiency and effectiveness of the IS environment in economic terms.

What is the skill set expected from an IS Auditor? Nov 2012
What are the responsibilities of an IS Auditor with regard to Controls?

Responsibility of IS Auditor:

The audit objective and scope require some set of skills that is generally expected from an IS auditor. It includes-

♦ Sound knowledge of business operations, practices and compliance requirements,
♦ Should possess the professional technical qualification and certifications,
♦ Good understanding of information Risks and Controls,
♦ Knowledge of IT strategies, Policy and procedure controls,
♦ Ability to understand technical and manual control,
♦ Good knowledge of Professional Standards and Best practices of IT controls.

Explain briefly the Functions of an IS Auditor in regard to Controls.
"IT Auditors review risks relating to IT systems & processes". Explain these briefly.

IT Auditor often is the communicator of IT related business risk, to management. He can check, understand, assess the risk and present risk-oriented advice to management. IT auditors review risks relating to IT systems and processes, some of the IT related risks, reviewed by auditor, are:

(i) Inadequate information security (ii) Inefficient use of corporate resources, or poor governance
(iii) Ineffective IT strategies, policies and practices (iv) IT-related frauds

Briefly explain some of the Audit Standards or Best Practices Standards related to IS Audit.

Following are some of the audit standards or best practices standards related to IS audit:

1. Audit Standards issued by ICAI: ICAI issues various standards and guidance notes in relation to audit. These standards can be helpful in IS audit also.

2. ISACA standards: ISACA (Information Systems Audit and Control Association) of USA has issued

- 16 IS audit standards which defines the mandatory requirements for IS auditing & reporting.
- 39 IS auditing guidelines which provide a guideline in applying IS auditing standards.
- 11 IS auditing procedure which provide examples of procedure an IS auditor need to follow while conducting IS audit.

3. COBIT (Control Objectives for information and related technology) - (Covered in Chapter 8)
4. ISO 27001: Information Security Management System - (Covered in Chapter 8)
5. ITIL (Information Technology Infrastructure library) - (Covered in Chapter 8)

6. Global Technology Audit Guide (GTAG): The Institute of Internal Auditors (IIA), USA, has issued GTAG which provides control and security guidelines in IT environment. Following is the list of GTAG developed by IIA.

- GTAG 1: Information Technology Controls
- GTAG 2: Change and Patch Management Controls
- GTAG 3: Continuous Auditing
- GTAG 4: Management of IT Auditing
- GTAG 5: Managing and Auditing Privacy Risks
- GTAG 6: Managing and Auditing IT Vulnerabilities
- GTAG 7: Information Technology Outsourcing
- GTAG 8: Auditing Application Controls
- GTAG 9: Identity and Access Management.

What Audit policy should do?
Suppose an IS audit policy is required, how will you lay down the responsibility of audit? May 2010

Note: First of all, write the scope of IS audit, thereafter write the following.

The audit may be conducted by internal or external auditor. IS auditor should be independent of the activities they audit. The Audit policy should essentially do the following -

(i) The Policy should lay out the periodicity of reporting and the authority to whom the reporting is to be made

(ii) A statement of professional proficiency may be included to state the minimum qualification and experience requirements of the auditors.

(iii) All information system auditors will sign a declaration of fidelity and secrecy before commencing the audit work in a form that the inspection department may design.

(iv) The policy may lay out the extent of testing to be done under the **various phases of the audit** like ***Planning, Compliance Testing, and Substantive Testing.***

(v) **You have been asked to conduct an IS Audit for a bank, how will you develop a documented audit program? Nov 2009**
What are the aspects to be included when a documented audit program is developed? Nov 2010

A documented audit program would be developed including the following:

- Documentation of the information system auditor's procedures for collecting, analyzing, interpreting, and documenting information during the audit.
- Objectives of the audit.
- Scope, nature, and degree of testing required to achieve the audit objectives in each phase of the audit.
- Identification of technical aspects, risks, processes, and transactions which should be examined.
- Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.

(vi) The policy should determine when and to whom the audit results would be reported and communicated. It would define the access rights to be given to the auditors. ***This access may include:***

- User level and/or system level access to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced transmitted or stored on respective Dept. equipment or premises;
- Access to work areas (labs, offices, cubicles, storage areas, etc.);
- Access to reports / documents created during internal audit;

- Access to interactively monitor and log traffic on networks.

(vii) The Policy should outline the compliance testing areas e.g.

- Organizational and Operational Controls;− Security Management Controls;
- System development and Documentation Controls;
- Application Controls;
- Physical and Environmental Controls;
- Access Controls;
- Business Continuity Controls, etc.

(viii) The auditor will carry out substantive testing wherever the auditor observes weakness in internal control or where risk exposure is high. The auditor may also carry out such tests to gather additional information necessary to form an audit opinion.

(ix) The Audit Policy would define the compulsory audit working papers to be maintained and their formats.

Write short notes on 'Audit Working Papers and Documentation'. Nov 2009

All significant matters which requires the judgment, together with the auditor's conclusion should be included in the working papers. **The form and contents of the working papers depends on -**

♦ The nature of the engagement.
♦ The form of the auditor's report.
♦ The nature and complexity of client's business.
♦ The nature and condition of client's records and degree of reliance on internal controls.

In case of recurring audits, some working paper files may be classified as ***permanent audit files*** which are updated with info of succeeding audit, as distinct from the ***current audit files*** which contain info ***relating*** primarily ***to audit of a single period***.

The permanent audit file normally includes -

♦ The organisation structure of the entity.
♦ The IS policies of the organization.
♦ The historical background of the information system.
♦ Extracts of copies of important legal document relevant to audit.
♦ A record of the study and evaluation of the internal controls.
♦ Copies of audit reports and observations of earlier years.
♦ Copies of management letters issued by the auditor.

The current file normally includes -

♦ Correspondence relating to the acceptance of appointment and the scope of the work.
♦ Document of the planning process of the audit and audit programme.
♦ A record of the nature, timing and extent of auditing procedures performed, and the results of each procedures.
♦ Copies of letters and notes concerning audit matters communicated or discussed with the client.
♦ Letters of representation and confirmation received from the client.
♦ Conclusions reached by the auditor concerning significant aspect of the audit.
♦ Copies on the data and system being reported on and the related audit reports.

Working papers are the property of the auditor. The auditor may, at his discretion, make portions of , or extracts from his working papers available to the client. The auditor should adopt reasonable procedures for custody and confidentiality of his working papers and should retain them for a period of time sufficient to meet the needs of his practice and satisfy any pertinent legal and professional requirements of record retention.

Discuss the parameters that would help in planning a documentation process of IS Audit. May 2012

The following three parameters would help in planning a documentation process:

1. The importance of planning and understanding the planning process: It requires identifying three planning questions:

a) **Knowing Your Resources:** The **3** basic resources: ***time***, ***people***, ***money***. One has to check for their availability and affordability.

b) **Defining the Scope and Audience:** The same report may undergo significant changes depending on the character of report and nature of audience. Presentation on Balance Sheet made to bankers and to investors would be quite different in content & focus.

c) **Using a Scope Definition Report:** It is critical to know how to complete a Scope Definition Report. This report helps in developing a workable schedule for completing the project.

2. The Documentation Writer: The qualities and skills that the documentation writer would need should be judged. The requirement may often be legal in nature.

3. Rules to guide documentation writing: ***The four rules of writing good documentation are*** -

a) **Writing in Active Voice:** Using active voice in documentation.

b) **Giving the Consequences:** Giving the consequences of the reader's action.

c) **Writing from General to Specific:** Designing the documentation from general to specific.

d) **Consistency:** Using of style, order and format consistently.

To get a good documentation of the working papers of an auditor, what are the points to be considered while gathering & organizing info and also mention the principles to be followed for writing the documentation. Nov 2010

In order to get a good documentation of the working papers of an auditor, the following ***points*** are ***to be considered during gathering of information:***

(i) **About the Reader:** Finding information about the reader by doing a task analysis. Three parts of the reader's task: viz. input, process, output will have to be identified before one could develop an understanding of a reader.

(ii) **About the Subject**: The three sources of information about a subject are people, paper, and the object of the report. **Organizing information**: It involves deciding what information to include and how to sequence it. The documentation should be

organized in such a manner that the reader can easily understand it and the various outcomes flowing from it should be clearly visible. Following are the ***points to be considered for organizing of information:***

(i) **Selecting Information:** Selecting 'what the reader needs to know'. Organizing the information into a useful sequence.

(ii) **Organizing the Documentation:** The sequence of document can be according to:-subject, difficulty, chronological, importance and analytical.

(iii) **Dividing Into Sections**: Dividing documentation into chapters or sections.

(iv) **Dividing Into Subsections:** Dividing sections or chapters into subsections.

Principles for writing the documentation: Following principles should be kept in mind for writing the documentation -

♦ **Writing in Active Voice:** Using active voice in documentation;

♦ **Giving the Consequences:** Giving the consequences of the reader's action;

♦ **Writing from General to Specific:** Designing the documentation from general to specific;

♦ **Consistency:** Using style, order & format consistently; and

♦ **Writing Online Documentation:** Laying down guidelines for writing online documentation by using appropriate techniques to emphasize text.

As an IS Auditor, what points you should consider while finalizing a document?

As an IS auditor, following points are to be considered for finalizing a document:

(i) **Reviewing and Testing:** Selection of reviewer of the documentation involves identification of subject and communication skill. The reviewer must be provided with adequate information regarding the audience and object of the report. In order to ensure objectivity It is recommended that the reviewer be a person who has not been involved in the documentation process.

(ii) **Generating the Glossary and Index:** Compilation of a glossary and generation of an index are two major tasks for a complete documentation. In order to achieve this task it is necessary to mark the Index and glossary entries at the stage of documentation itself. Word processing software comes with an inbuilt ability of creating an index from the identified text in the body of the document.

(iii) **Formatting and Production:** The idea of creating a good document is not possible without first deciding on a good design for the same. This involves choosing effective formatting options for headings, sub-headings, section breaks, formatting, & allied.

(iv) **Appropriate binding style:** It is also important to select an appropriate binding style that would aid filing & ease of consultation.

As an IS Auditor, discuss the various contents in brief to be included in a standard audit report. Nov 2008, May 2011

Audit reports broadly include the following sections -

1. Cover and Title Page: Audit reports should use a standard cover, with a window showing the title: ***"Info System Audit"*** or ***"Data Audit"***, The department's name and the report's date of issue. The title page may also indicate the names of the audit team members.

2. Table of Contents: The table lists the sections and sub-sections with page numbers including summary and recommendations.

3. Summary/Executive Summary: The summary gives a quick overview of the salient features at the audit in. It should not normally exceed ***3 pages***, including the recommendations.

4. Introduction: Since the readers will read the summary, the introduction should not repeat the details. It should include the following elements -

- **Context:** This sub-section briefly describes the entity's role, size and organisation especially with regard to information system management, significant pressures on info system management during the period under review, events that need to be noted, results of internal audits.
- **Purpose:** This sub-section is a short description of what functions and special programs were audited and the clients' authorities.
- **Scope:** The scope lists the period under review, the issues covered in each function & program, the locations visited & the on-site dates.
- **Methodology:** This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology.

5. Findings: It constitutes the main part of an audit report. They result from the examination of each audit issue in the context of objectives and clients' expectations. If the auditor is using any standard grading, the arrived value should also be stated.

6. Opinion: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.

7. Appendices: Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

What are the general guidelines to be followed while preparing IS Audit Report?

1. Level of Detail: The depth of coverage for issues should normally reflect the significance of the findings. Situations representing a high degree of risk or indicating shortcomings that are serious enough to justify a recommendation should be treated extensively. Specific initiatives that the auditors wish to mention as examples should be described in detail, while issues where the department meets the expectations and there is nothing specific to mention should be dealt with briefly.

2. Commentary: Where a recommendation and a compliment are made under the same issue, they should be in separate paragraphs; otherwise, they may confuse the reader and reduce the impact of one or the other.

3. Use of Statistics: Statistics need to be used consistently throughout the report. Sample size and error rate mean more when they are given in context. The size of the population, the number of transactions and the period of time provide that context. *Percentages should not be used when referring to small samples* (less than one hundred). Graphics should be used when they add to the understanding of the text.

What are the major aspects that should be covered while drafting IS Security Policy for End-user Computing Policies in detail? RTP May 2014

Major aspects that should be covered while drafting IS Security Policy for end user computing policies are given as follows:

1. Approval for End-User Production System Development Efforts: All software that handles sensitive, critical, or valuable information and that has been developed by end-users must have its controls approved by the information security function prior to being used for production processing.

2. When Making Additional Copies of Software is Permissible: Third-party software in the possession of the organization must not be copied unless such copying is consistent with relevant license agreements and unless management has previously approved of the copying or copies are being made for contingency planning purposes.

3. Games May Not Be Stored or Used on Computer Systems: Games may not be stored or used on any computer systems.

4. Initial Backup Copies of Microcomputer Software: All microcomputer software must be copied prior to its initial use, and the copies must be stored in a safe place. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard-disk crashes, and other computer problems. These master copies must also be stored in a secure location.

5. Periodic Review of Software Licensing Agreements: The agreements for all computer programs licensed from third parties must be periodically reviewed for compliance.

6. Storage of Sensitive Information on Personal Computers: If sensitive information is to be stored on the hard- disk drive or other internal components of a personal computer, it must be protected by either a physical lock or encryption. If this information is written to a floppy disk, magnetic tape, smart card, or other storage media, the media must be suitably marked with the highest relevant sensitivity classification. When not in use, these media must be stored in locked furniture.

Note: ***Please Refer Study Material for*** **'Sample IS security policy'.**

CHAPTER 10 - INFORMATION TECHNOLOGY (AMENDMENT) ACT 2008

Write short notes on Objectives of Information Technology Act, 2000. May 2012

Objectives of the Act are:

1) 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.
2) To give legal recognition to Digital signatures for authentication of any information or matter which requires authentication under any law.
3) To facilitate electronic filing of documents with Government departments.
4) To facilitate electronic storage of data.
5) To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions.
6) To give legal recognition for keeping of books of accounts by banker's in electronic form.
7) 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.

CHAPTER-I: PRELIMINARY

Explain briefly the Scope of ITAA 2008 along with the relevant definitions that are used. Practice Manual

Scope of ITAA 2008:

Section 1: Short Title, Extent, Commencement and Application

Sec 1(1) - This act may be called IT Act, 2000. [As amended by IT (Amendment) Act 2008]

Sec 1(2) - It shall extend to whole of India and save as otherwise provided in this act, It applies also to any offence or contravention hereunder committed o/s India by any person.

Sec 1(3) - The Act was enforced by the CG from October 17, 2000.

***The Act shall not apply to the following*:**

Sec 1(4) - Nothing in this act shall apply to documents or transactions specified in the first schedule by way of addition or deletion of entries thereto. These are -

1. A negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
2. A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
3. A trust as defined in section 3 of the Indian Trusts Act, 1882;
4. A will as defined in Indian Succession Act, 1925;
5. Any contract for the sale or conveyance of immovable property or any interest in such property;
6. Any such class of documents or transactions as may be notified by the CG in the official gazette.

Sec 1(5) - Every notification issued u/s 1(4) shall be laid before each House of Parliament.

Note: ***Refer next question for relevant definitions used under ITAA 2008.***

List some important definitions provided under IT Act, 2000. V.Imp.

Section 2: Definitions

Section 2(1) In this Act, unless the context otherwise requires,

Sec.2(1)(a) "Access" with its grammatical variations & cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

Sec.2(1)(b) "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

Sec.2(1)(c) "Adjudicating Officer" means adjudicating officer appointed u/s 46(1);

Sec.2(1)(d) "Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature;

Sec.2(1)(e) "Appropriate Government" means as respects any matter -

(i) enumerated in List II of the Seventh Schedule to the Constitution;

(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government;

Sec.2(1)(f) "Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

Sec.2(1)(g) "Certifying Authority" means a person who has been granted a license to issue a ESC u/s 24;

Sec.2(1)(h) "Certification Practice Statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;

Sec.2(1)(ha) "Communication Device" means Cell Phones, Personal Digital Assistance, or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image.

Sec.2(1)(i) "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

Sec.2(1)(j) "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through -

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

(ii) terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained;

Sec.2(1)(k) "Computer Resource" means computer, communication device, computer system, computer network, data, computer database or software;
Sec.2(1)(l) "Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
Sec.2(1)(m) "Controller" means the Controller of Certifying Authorities appointed u/s 17(7);
Sec.2(1)(n) "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal established u/s 48(1);
Sec.2(1)(na) "Cyber Café" means 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.
Sec.2(1)(nb) "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.
Sec.2(1)(o) "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
Sec.2(1)(p) "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;
Sec.2(1)(q) "Digital Signature Certificate" means a Digital Signature Certificate issued u/s 35(4) ;
Sec.2(1)(r) "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
Sec.2(1)(s) "Electronic Gazette" means official Gazette published in the electronic form;
Sec.2(1)(t) "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;
Sec.2(1)(ta) "Electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature
Sec.2(1)(tb) "Electronic Signature Certificate" means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate"
Sec.2(1)(u) "Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;
Sec.2(1)(ua) "Indian Computer Emergency Response Team" means an agency established u/s 70 B(1).
Sec.2(1)(v) "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;
Sec.2(1)(w) "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.
Sec.2(1)(x) "Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;
Sec.2(1)(y) "Law" includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws & orders issued or made there under
Sec.2(1)(z) "License" means a license granted to a Certifying Authority u/s 24;
Sec.2(1)(za) "Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;
Sec.2(1)(zb) "Prescribed" means prescribed by rules made under this Act;
Sec.2(1)(zc) "Private Key" means the key of a key pair used to create a digital signature;
Sec.2(1)(zd) "Public Key" means the key of a key pair used to verify a digital signature and listed in the DSC;
Sec.2(1)(ze) "Secure System" means computer hardware, software, and procedure that -
(a) are reasonably secure from unauthorized access and misuse;
(b) provide a reasonable level of reliability and correct operation;
(c) are reasonably suited to performing the intended functions; and
(d) adhere to generally accepted security procedures;
Sec.2(1)(zf) "Security Procedure" means the security procedure prescribed under section 16 by the Central Government;
Sec.2(1)(zg) "Subscriber" means a person in whose name the Electronic Signature Certificate is issued;
Sec.2(1)(zh) "Verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether
(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

Section 2(2) - Any reference in this act to any enactment or any provision thereof shall, in relation to an area, in which such enactment or such provision is not in force, be construed as a reference to the corresponding law or the relevant provision of the corresponding law, if any, in force in that area.

CHAPTER-II: DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature? What is a Digital Signature? How is created and used? Practice Manual, Nov 2009

Meaning of Digital Signature Certificate: A DSC is a mechanism for authenticating & securing the info that is transmitted b/w the two parties. It is simply a public key, along with some identifying info, that has been digitally signed by a Certifying Authority. It identifies the subscriber, CA, & its operational period and contains the subscriber public key. The DSC ensures that the purported sender is in fact the person who sent the message. The certificate is thus protected so that it can't be altered without detection.

Legal Definition: "Digital Signature" [Sec.2(1)(p)] means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Section 3 deals with the conditions subject to which an electronic record may be authenticated by means of affixing digital signature which is created in two distinct steps. These are -

Step 1 - The electronic record is converted into a ***message digest*** by using a mathematical function known as "***Hash Function***" which digitally freezes the electronic record, thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tempering with the contents of the electronic record will immediately invalidate the digital signature.

Step 2 - The identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest & which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tempered 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.

Write short notes on 'Authentication of Electronic Records' u/s 3 of IT Act 2008. Jun & Nov 09, M 11, RTP M 13, N 13

Section 3: Authentication of Electronic Records:

Sec. 3(1) Subject to the provisions of this section any subscriber may authenticate an e-record by affixing his Digital Signature.

Sec. 3(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.

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

Sec. 3(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Write short notes on 'Electronic Signature' given u/s 3A of ITAA 2008. RTP May 2012

"Electronic signature" [Sec.2(1)(ta)] means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature

Sec. 3A(1) Notwithstanding anything contained in section 3, but subject to the provisions of subsection (2) a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which:

(a) is considered reliable ; and

(b) may be specified in the Second Schedule

Sec. 3A(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or , as the case may be, the authenticator and of no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfills such other conditions which may be prescribed.

Sec. 3A(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated

Sec. 3A(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule; Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable

Sec. 3A(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament

CHAPTER-III: ELECTRONIC GOVERNANCE

Bring out the legal recognition granted to electronic records, contracts formed through electronic means and digital signatures. Nov 2009

Section 4: Legal Recognition of Electronic Records:

Where any law provides that info or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is –
(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference

Section 10 A: Validity of contracts formed through electronic means (explained later in this chapter)

Section 5: Legal recognition of Electronic Signature:

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then,notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation – For the purposes of this section, **"Signed"**, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "Signature" shall be construed accordingly.

Write short notes on 'use of electronic records & electronic signature in Govt. & its agencies'. RTP Nov 09, RTP May 14

Section 6: Use of Electronic Records and Electronic Signature in Government and its agencies:

Sec. 6(1) Where any law provides for –
(a) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
(b) the issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
(c) the receipt or payment of money in a particular manner, then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

Sec. 6(2) The appropriate Government may prescribe rules for the purposes of sub-section (1), by rules, prescribe
(a) the manner and format in which such electronic records shall be filed, created or issued;
(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

"Appropriate Government" [Sec.2(1)(e)] - (Given in definitions)

Do also explain Section 9 - (Given below)

Explain the provisions relating to delivery of services by service provider.

Section 6A: Delivery of Services by Service Provider :

Sec 6A(1) - ***The appropriate Government may***, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means ***authorize***, by order, ***any service provider*** to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

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

Sec 6A(2) - The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

Sec 6A(3) - Subject to the provisions of sub-section (2), the appropriate Government may authorize the service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate service charges by the service providers.

Sec 6A(4) - Appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section Provided that the appropriate Government may specify different scale of service charges for different types of services.

What are the conditions laid down under IT Act, 2000 regarding 'Retention of Electronic Records'?
May 2010, May2012, RTP May 2013

"Electronic Record" [Sec.2(1)(t)] means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

Section 7: Retention of Electronic Records: This section deals with the conditions for retention of electronic records.

Sec 7(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, provided, the following conditions are satisfied:
(a) the information contained therein remains accessible so as to be usable for a subsequent reference;
(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.
However, this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Sec 7(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.

Do also explain Section 9 - (Given below)

Write short notes on 'Audit of Documents etc in Electronic Form'.

Section 7A: Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

What is an Electronic Gazette? Can publication be made in the Electronic Gazette? RTP May 2010

"Electronic Gazette" [Sec.2(1)(s)] means official Gazette published in the electronic form

Section 8: Publication of Rules, Regulation, etc, in Electronic Gazette:

Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette:However, where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

Section 9: Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form:

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

Describe the Powers to make rules by Central Government in respect of Electronic Signature u/s 10 of ITAA 2008. May 2012, RTP Nov 2013, RTP May 2014

Section 10: 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 & procedures to ensure adequate integrity, security & confidentiality of electronic records or payments; and

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

Briefly explain the validity given by IT Act to the contracts formed through electronic means.

Section 10A: Validity of contracts formed through electronic means :

Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

How does the ITAA 2008 enable the objective of the Govt. in spreading e-governance? Nov 2009

In ITAA 2008, Chapter III is related with the objective of the govt. in spreading e-governance. It deals with the procedures to be followed for sending & receiving of e-records. This chapter contains sections 4 to 10.

Note: ***Now briefly discuss sections 4 to 8.***

Discuss the main provisions provided in ITAA 2008 to facilitate E-Governance. Practice Manual

E-Governance sections 6 to 8 of Chapter III are the main sections for provisions related to E-governance provided in ITAA 2008 to facilitate e-governance.

Note: ***Now briefly discuss sections 6 to 8.***

CHAPTER-IV: ATTRIBUTION, ACKNOWLEDGMENT AND DISPATCH OF ELECTRONICRECORDS

Discuss the provisions relating to attribution and acknowledgment of electronic records. RTP Nov 2010, Nov 2010

Section 11: This Section deals with **Attribution of Electronic Records; viz**

An electronic record shall be attributed to the originator

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

Where **"Originator" [Sec.2(1)(za)]** means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary

Section 12: This Section deals with **Acknowledgment of Receipt of electronic records.**

Sec 12(1) - Where the originator has not stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

Sec 12(2) - Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

Sec 12(3) - Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

Discuss the provisions relating to time and place of dispatch of electronic records.

Section 13 deals with the time and place of dispatch and receipt of electronic record.

Sec 13(1) - Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
Sec 13(2) - Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely –
(a) if the addressee has designated a computer resource for the purpose of receiving electronic records
(i) receipt occurs at the time when the electronic record enters the designated computer resource; or
(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee
(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.
Sec 13(3) - Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to "be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
Sec 13(4) - The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
Sec 13(5) - For the purposes of this section -
(a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;
(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
(c) "Usual Place of Residence", in relation to a body corporate, means the place where it is registered.

CHAPTER-V: SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES

What does the IT Act, 2008 say about 'Secure Electronic Signature' in Section 15? Nov 2010, RTP Nov 2013

Section 14: Secure Electronic Record: Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.
Section 15: Secure Electronic Signature : An electronic signature shall be deemed to be a secure electronic signature if-
(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory & no other person; and
(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed
Explanation – In case of digital signature, the "signature creation data" means the private key of the subscriber
Section 16: Security procedures and Practices : The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices ***Provided that*** in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

CHAPTER-VI: REGULATION OF CERTIFYING AUTHORITIES

Explain the provisions relating to 'Appointment of Controller & Other Officers' in IT Act.

Section 17: The provisions relating to the appointment of Controller & other officers to regulate the Certifying Authorities are hereunder:
1. The CG may, by notification in the official gazette, appoint a controller of certifying authorities for the purposes of this Act and may also by the same time or subsequent notification appoint such no. of Deputy Controllers (DC) & Assistant Controllers (AC), other officers & employees as it deems fit.
2. The Controller shall discharge his functions under this Act subject to the general controls & directions of the CG.
3. The DC & AC shall perform the functions assigned to them by the Controller under the general superintendence & control of the Controller.
4. The qualifications, experience and terms & conditions of the service of Controller, DC & AC shall be as such as may be prescribed by the CG.
5. The H.O and B.O of the office of the Controller shall be at such places as the CG may specify, and these may be established at such places as the CG may think fit.

Explain briefly what are the functions that a Controller may perform. RTP May 2013, Nov 2013

Section 18: Functions of Controller: The Controller may perform all or any of the following functions, namely:
(i) certifying public keys of the Certifying Authorities
(ii) laying down the standards to be maintained by the Certifying Authorities;
(iii) laying down the duties of the Certifying Authorities;
(iv) exercising supervision over the activities of the Certifying Authorities;
(v) specifying the qualifications and experience which employees of the Certifying Authorities should possess;
(vi) specifying the conditions subject to which the Certifying Authorities shall conduct their business;
(vii) specifying the content of written/printed /visual material & advertisements that may be used in respect of ESC & Public Key;
(viii) specifying the form and content of a Electronic Signature Certificate and the key;
(ix) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
(x) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
(xi) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
(xii) resolving any conflict of interests between the Certifying Authorities and the subscribers;

Other functions/Powers:

Section 27: Power to delegate - The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

Section 28: Power to investigate contraventions - The Controller or any officer authorized by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.

Section 29: Access to computers and data - The controller or any person authorized by him, shall have access to any computer system, data or any other material connected with such system if he has reasonable cause to suspect that any contravention of the provisions of this chapter has been committed.

Write short notes on 'Recognition of Foreign Certifying Authorities' u/s 19 of ITAA 2008. May 13, RTP May 14

Section 19: Recognition of foreign Certifying Authorities:

Sec 19(1) - Subject to such conditions & restrictions as may be specified by regulations, ***the Controller may*** with the previous approval of the CG, and by notification in the official gazette, ***recognize any foreign authority as a certifying authority*** for the purposes of this Act.

Sec 19(2) - Where any certifying authority is recognized u/s 19(1), ***the electronic signature certificate*** issued by such certifying authority ***shall be valid*** for the purposes of this Act.

Sec 19(3) - ***The Controller may*** if he is satisfied that any certifying authority has contravened any of the conditions & restrictions subject to which it was granted recognition u/s 19(1), he may, for reasons to be recorded in writing, by notification in the official gazette, ***revoke such recognition***.

Discuss the conditions to be satisfied by a person for obtaining a license to issue electronic signature certificates.

Section 21: License to issue electronic signature certificates:

Sec 21 (1) - Subject to the provisions of sub-section (2), any person may make an application, to the controller, for a license to issue electronic signature certificates.

Sec 21 (2) - No license shall be issues under sub-section (1), unless the applicant fulfills such requirements w.r.t qualification, expertise, manpower, financial resources, and other infrastructure facilities, which are necessary to issue electronic signature certificates as may be prescribed by the CG.

Sec 21 (3) - A license granted under this section shall -

a) be valid for such period as may be prescribed by the CG;
b) not be transferable or heritable;
c) be subject to such terms & conditions as may be specified by the regulations.

Explain the procedure to apply for the license to issue electronic signature certificates u/s 22 of IT Act. May 2013

Section 22: Application for license:

Section 22 provides that the application for licence shall be accompanied by a certification practice statement and statement including the procedure with respect to identification of the applicant. It shall be further accompanied by a fee not exceeding **Rs.25,000** and other documents as may be prescribed by the Central Government.

Section 23: Renewal of license:

Section 23 provides that the application for renewal of a licence shall be in such form and accompanied by such fees not exceeding **Rs.5,000** which may be prescribed by the Central Government.

Section 24: Procedure for grant or rejection of license:

Section 24 deals with the procedure for grant or rejection of license by the controller on certain grounds. No application shall be rejected under this section **unless** the applicant has been given a reasonable opportunity of presenting his case.

In IT Act, what do sec 25 & 26 say about suspension of a license to issue electronic signature certificates? Nov 2012

Section 25: Suspension of License:

Section 25 provides that the Controller may revoke a license on grounds such as incorrect or false material particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made there under.

However, no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

Also, no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

Section 26: Notice of suspension or revocation of license:

As per Sec 26, the Controller shall publish a notice of suspension or revocation of license as the case may be in the database maintained by him. Further, the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock. It is also provided that the Controller may, if he considers necessary, publicize the contents of database in such electronic or other media, as he may consider appropriate.

Note: ***Also give section 33 with these sections.***

Describe the Duties of Certifying Authority i.r.o Digital Signature u/s 30 of ITAA 2008.
Nov 2010, May 2011, RTP May 12, RTP Nov 2012, Nov 2012

Section 30: Duties of Certifying Authorities - Every Certifying Authority shall –

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse:
(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
(c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured
(ca) be the repository of all Electronic Signature Certificates issued under this Act
(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and
(d) observe such other standards as may be specified by regulations.

Section 31: Certifying Authority to ensure compliance of the Act, etc. - Every CA shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement with the provisions of this Act, rules, regulations & orders made there under.

Section 32: Display of license - Every CA shall display its licence at a conspicuous place of the premises in which it carries on its business.

Section 33: Surrender of license -

Sec 33(1) - Every CA whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

Sec 33(2) - Where any CA fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence & shall be punished with ***imprisonment*** which ***may extend upto 6 months*** or a ***fine*** which ***may extend to Rs. 10,000*** **or** ***with both***.

Section 34: Disclosure -

Sec 34(1) - Every CA shall disclose in the manner specified by regulations:

(a) its Electronic Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of revocation or suspension of its own digital certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a ESC, which that Authority has issued, or the Authority's ability to perform its services

Sec 34(2) - Where in the opinion of the CA any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a ESC was granted, then, the CA shall –

(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

What are the regulations relating to the appointment & powers of the CA under Chapter VI, sections 17 to 25 of ITAA 2008? Practice Manual

Note: ***Refer above sections.***

CHAPTER-VII: ELECTRONIC SIGNATURE CERTIFICATES

Mention the provisions relating to issue of Digital/Electronic Signature Certificates. Nov 2003

Section 35: Certifying Authority to issue Electronic Signature Certificate - This section lays down the procedure for issuance of a Digital Signature Certificate. It provides that an application for such certificate shall be made in the prescribed form and shall be accompanied by a **fee not exceeding Rs.25,000**. The fee shall be prescribed by the Central Government, and different fees may be prescribed for different classes of applicants.

The section also provides that ***No Digital Signature Certificate shall be granted unless*** the CA is satisfied that –

(a) the applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

Section 36 : Representations upon issuance of Digital Signature Certificate

Section 36 required that while issuing a Digital Signature Certificate, the Certifying Authority should certify that it has complied with the provisions of the Act, the rules and regulations made there under and also with other conditions mentioned in the DSC.

Explain the provisions relating to suspension or revocation of Digital Signature Certificate.

Section 37: Suspension of Digital Signature Certificate - The CA may suspend such certificate if it is of the opinion that such a step needs to be taken in public interest. Such certificate shall not be suspended for a period exceeding **15 days** unless the subscriber has been given an opportunity of being heard.

Section 38: Revocation of Digital Signature Certificate - This Section provides for the revocation of DSC under certain circumstances. Such ***revocation shall not be done unless*** the subscriber has been given an ***opportunity of being heard*** in the matter. Upon revocation or suspension the CA shall publish the notice of suspension or revocation of a DSC.

Section 39: Notice of suspension or revocation -

(1) Where a DSC is suspended or revoked **u/s 37 or 38**, the CA shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the DSC for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

CHAPTER-VIII: DUTIES OF SUBSCRIBERS

State the Duties of the Subscriber of a Digital Signature certificate as specified in Sections 40 to 42 of Chapter VIII of ITAA 2008. Practice Manual

Section 40: Generating Key Pair - Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, the subscriber shall generate that key pair by applying the security procedure.

Section 40A: Duties of subscriber of Electronic Signature Certificate - In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.

Describe the 'Acceptance of Digital Signature Certificate' w.r.t section 41 of ITAA 2008. Nov 2010, RTP Nov 12 & 13

Section 41: Acceptance of Digital Signature Certificate:

Sec 41(1) - A subscriber shall be deemed to have accepted a DSC if he publishes or authorizes the publication of a DSC -

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the DSC in any manner.

Sec 41(2) - By accepting a DSC the subscriber certifies to all who reasonably rely on the information contained in the DSC that –

(a) the subscriber holds the private key corresponding to the public key listed in the DSC and is entitled to hold the same;

(b) all representations made by the subscriber to the CA and all material relevant to the information contained in the DSC are true;

(c) all information in the DSC that is within the knowledge of the subscriber is true.

Section 42: Control of Private key:

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation – For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CHAPTER-IX: PENALTIES AND ADJUDICATION

Explain the 'Penal Provisions' with reference to ITAA 2008. Practice Manual

Sections 43 to 45 of Chapter IX of ITAA 2008 deal with different nature of penalties. These are -

Section 43: Penalty and Compensation for damage to computer, computer system, etc. - A person shall be liable to pay compensation if he, without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data from such system or network;

(c) introduces computer contaminant or computer virus into the system or network;

(d) damages data or computer system or computer network;

(e) disrupts computer, computer system or computer network;

(f) denies access to any authorized person to access any computer system or computer network;

(g) wrongly charges the services availed of by a person to the another person;

(h) destroys, deletes or alters any information residing in a computer resource;

(i) Steals, conceals, destroys or alters source code

Explanation - for the purposes of this section -

(i) **"Computer Contaminant"** means any set of computer instructions that are designed -

(a) to modify, destroy, record, transmit data or programme residing within a computer,computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) **"Computer Database"** means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) **"Computer Virus"** means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) **"Damage"** means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

(v) **"Computer Source code"** means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form

Section 43A: Compensation for failure to protect data - If an organization possess, deal or handle any sensitive personal data or information in its computer resource, then if it is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes loss to any person, then such organization shall be liable to pay damages by way of compensation, to the person so affected.

Section 44: Penalty for failure to furnish information, return, etc. - ***If any person who is required*** under this Act or any rules or regulations made there under ***to***:

(a) ***furnish any document, return or report to the Controller or the CA*** **:** fails to furnish the same, he shall be liable to a penalty not exceeding **Rs. 1,50,000** for each such failure

(b) ***file any return or furnish any information, books or other documents within the time specified*****:** fails to file return or furnish the same within the time specified, he shall be liable to a penalty not exceeding **Rs. 5,000** for every day during which such failure continues

(c) ***maintain books of account or records*****:** fails to maintain the same, he shall be liable to a penalty not exceeding R**s. 10,000** for every day during which the failure continues.

Section 45: Residuary Penalty - This section provides for residuary penalty. Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation/penalty not exceeding **Rs. 25,000**.

Explain the Powers of Adjudicating Officer as given u/s 46 of ITAA 2008, while adjudicating the matters relating to claim for injury or damages to computer, computer system, computer network or computer resource etc.

Section 46: Power to Adjudicate -

Sec 46(1) - For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under which renders him liable to pay penalty or compensation, the CG shall, ***subject to the provisions of sub-section(3)***, appoint any officer not below the rank of a Director to

the Government of India or an equivalent officer of a SG to be an adjudicating officer for holding an inquiry in the manner prescribed by the CG.

Sec 46(1A) - The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed **Rs. 5 crores**.

Provided that the jurisdiction in respect of claim for injury or damage exceeding **Rs. 5 crores** shall vest with the competent court.

Sec 46(2) - The adjudicating officer shall, after giving the person referred to in subsection (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty as he thinks fit in accordance with the provisions of that section.

Sec 46(3) - No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of IT and Legal or Judicial experience as may be prescribed by the CG.

Sec 46(4) - Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

Sec 46(5) - Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal u/s 58(2) , and –

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of ***sections 193 and 228*** of the Indian Penal Code;

(b) shall be deemed to be a civil court for the purposes of ***sections 345 and 346*** of the Code of Criminal Procedure, 1973.

(c) shall be deemed to be a Civil Court for purposes of order XXI of the Civil Procedure Code, 1908.

What factors are to be taken by the Adjudicating Officer u/s 47 of ITAA 2008 while adjudging the quantum of compensation?

Section 47: Factors to be taken into account by the adjudicating officer - While adjudging the quantum of compensation the adjudicating officer shall have due regard to the following factors, namely -

(a) the amount of gain or unfair advantage made as a result of the default

(b) the amount of loss caused to any person as a result of the default

(c) the repetitive nature of the default

CHAPTER-X: THE CYBER APPELLATE TRIBUNAL

Describe the Composition and Powers of Cyber Regulatory Appellate Tribunal. Nov 2011

As per ITAA 2008, the Cyber Regulation Appellate Tribunal shall consist of one person called the **'Presiding Officer'** of the Tribunal who shall be appointed by the CG. Such a person must be qualified to be a judge of a High Court or is or has been a member of the Indian Legal Service in the post in Grade I of that service for at least **3 years.**

The Presiding Officer shall hold office for a term of **5 years** or upto a maximum age limit of **65 years**, ***whichever is earlier.***

Note - Powers of Cyber Regulatory Appellate Tribunal: ***Refer Section 58(2) given in following sections.***

Discuss the Composition of Cyber Appellate Tribunal u/s 49 of ITAA 2008. RTP Nov 2012

Sec.2(1)(n) "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal established u/s 48(1)

Section 48: Establishment of Cyber Appellate Tribunal -

(1) The CG shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.

(2) The CG shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Section 49: Composition of Cyber Appellate Tribunal -

Sec 49(1) - The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the CG may, by notification in the Official Gazette, appoint .

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the ITAA 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the ITAA 2008.

Sec 49(2) - The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India.

Sec 49(3) - Subject to the provisions of this Act-

(a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof

(b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.

Provided that every Bench shall be presided over by the Chairperson or the Judicial Member appointed u/s of 50(3)

(c) ***the Benches*** of the Cyber Appellate Tribunal ***shall sit at New Delhi*** and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify.

(d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction.

Sec 49(4) - Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench

Sec 49(5) - If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench a the Chairperson may deem fit.

What Qualifications are required for Appointment as Chairperson and Members of Cyber Appellate Tribunal?

Section 50: Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal -

(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a ***Judge of a High Court***;
(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having ***special knowledge*** of **and** ***professional experience in IT***, telecommunication, industry, management or consumer affairs.
Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the CG or a SG, and has held the post of Additional secretary to the Government of India or any equivalent post in the CG or SG for a period of not less than two one years or joint secretary to the Government of India or any equivalent post in the CG or SG for a period of not less than **7 years**.
(3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a ***member of the Indian Legal Service*** **and** ***has held the post of Additional Secretary*** for a period of not less than **1 year or** ***Grade I post of that service*** for a period of not less than **5 years**.

Explain the term of office, conditions of service etc of Chairperson and Members of Cyber Appellate Tribunal.

Section 51: Term of office, conditions of service etc of Chairperson and Members -
(1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of **5 years** from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier.
(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.
(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member.
Section 52 provides for the salary and allowances and other terms and conditions of service of the presiding Officer.
Section 52: Salary, allowance and other terms and conditions of service of Chairperson and Member -
The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of Cyber Appellate Tribunal shall be such as may be prescribed:
Section 52A: Powers of superintendence, direction, etc -
The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.
Section 52B: Distribution of Business among Benches -
Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.
Section 52C: Powers of the Chairperson to transfer cases -
On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or suo motu without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.
Section 52D: Decision by majority -
If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.

Who may fill the vacancy in the office of Chairperson or the Member of Cyber Appellate Tribunal in case there is vacancy for a reason other than temporary absence?

[Section 53] Filling up of vacancies :
If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson or Member as the case may be of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

Explain the procedure relating to resignation & removal of the Chairperson or Member of the Cyber Appellate Tribunal.

[Section 54] Resignation and removal :
(1) The Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:
However, the said Chairperson or Member shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of **3 months** from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, **whichever is earliest**.
(2) The Chairperson or Member of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved mis-behaviour or incapacity after an inquiry made by a Judge of the Supreme Court in which the Chairperson or Member concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.
(3) The Central Government may, by rules, regulate the procedure for the investigation of mis-behaviour or incapacity of the aforesaid Chairperson or Member.
[Section 55] Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings :

No order of the Central Government appointing any person as the Chairperson or Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

Briefly discuss about the staff of the Cyber Appellate Tribunal u/s 56 of ITAA 2008.

[Section 56] Staff of the Cyber Appellate Tribunal (Error in amendment...item 28) :

(1) The CG shall provide the Cyber Appellate Tribunal with such officers and employees as the Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries and allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

Explain the provisions relating to Appeal to Cyber Regulations Appellate Tribunal.

Section 57: Appeal to Cyber Regulations Appellate Tribunal -

1) Any person aggrieved by an order made by a Controller or an adjudicating officer may file an appeal to a Cyber Appellate Tribunal.

2) If the adjudicating officer made an order with the consent of the parties then appeal against such order cannot be filed.

3) Appeal can be filed within **45 days** from the date of receipt of order of controller or adjudicating officer. **However,** Appeal can be accepted after 45 days if there is sufficient cause for the delay.

4) The appeal has to be filed in prescribed form, together with the prescribed fees.

5) After giving the parties an opportunity of being heard, the tribunal will pass such orders as it thinks fit, confirming, modifying or setting aside the order appealed against.

6) The appeal shall be decided as early as possible and an effort shall be made to finish the appeal within **6 months**.

Write short notes on 'Powers of Cyber Appellate Tribunal'. Nov 2008

Section 58: Procedure and Powers of the Cyber Appellate Tribunal:

Sec 58 (1) - The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act & of the rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

Sec 58 (2) - *The Cyber Appellate Tribunal shall have*, for the purposes of discharging their functions under this Act, *the same powers* as are vested in a civil court under the Code of Civil Procedure, while trying a suit, in respect of the following matters, -

(i) Summoning and enforcing the attendance of any person and examining him on oath;

(ii) Requiring the discovery and production of documents or other electronic records;

(iii) Receiving evidence on affidavits;

(iv) Issuing commissions for the examination of witnesses or documents;

(v) Reviewing its decisions;

(vi) Dismissing an application for default or deciding it ex-parte;

(vii) Any other matter which may be prescribed.

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of **sec 193 & sec 228**, and for the purposes of **sec 196** of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of **sec 195** and **chapter XXVI** of the Code of Criminal Procedure, 1973.

Whether Civil Court has jurisdiction to entertain any suit or proceeding i.r.o any matter which an adjudicating officer is empowered to determine?

[Section 61] Civil court not to have jurisdiction :

No court shall have jurisdiction to entertain any suit or proceeding ***in respect of any matter which an adjudicating officer*** appointed under this Act or the Cyber Appellate Tribunal constituted under this Act ***is empowered*** by or under this Act ***to determine*** **and** ***no injunction shall be granted by any court*** or other authority ***in respect of any action taken*** or to be taken in pursuance of any power conferred by or ***under this Act***.

Provided that the court may exercise jurisdiction in cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter.

Can Appeal be made to High Court against the order of Cyber Appellate Tribunal?

Section 62: Appeal to High court:

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court ***within 60 days from the date of communication of the decision or order of the Cyber Appellate Tribunal*** to him on any **question of fact or law** arising out of such order. **However**, the ***High Court may***, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, ***allow*** it to be filed within ***a further period not exceeding 60 days***.

Explain the provisions relating to 'Compounding of Contravention' u/s 63 of ITAA 2008.

[Section 63] Compounding of Contravention :

(1) Any contravention under this Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be specially authorized by him in this behalf or by the adjudicating officer, as the case may be, subject to such conditions as the Controller or such other officer or the adjudicating officer may specify:

However, such sum shall not, in any case, exceed the maximum amount of the penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) shall apply to a person who commits the same or similar contravention within a period of **3 years** from the date on which the first contravention, committed by him, was compounded.

Explanation - For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of **3 years** from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1), no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

What is the provision in ITAA, if an imposed penalty or awarded compensation is not paid?

[Section 64] Recovery of Penalty or compensation :

A penalty imposed or compensation awarded under this Act, if it is not paid, shall be recovered as an arrear of land revenue and the license or the Electronic Signature Certificate, as the case may be, shall be suspended till the penalty is paid.

CHAPTER-XI: OFFENCES

What are the Offences and related Penalities under Chapter XI of ITAA 2008?

Section	Offence	Penalty
65	Tampering with Computer Source Documents	Imprisonment upto 3 years or fine upto 2 lacs or both
66	Computer Related Offences as per section 43	Imprisonment upto 3 years or fine upto 5 lacs or both
66A	Sending offensive messages through communication service, etc	Imprisonment upto 3 years and fine
66B	Dishonestly receiving stolen computer resource or communication device	Imprisonment upto 3 years or fine upto 1 lacs or both
66C	Identity theft	Imprisonment upto 3 years or fine upto 1 lacs or both
66D	Cheating by personating by using computer resource	Imprisonment upto 3 years or fine upto 1 lacs or both
66E	Violation of privacy	Imprisonment upto 3 years or fine upto 2 lacs or both
66F	Cyber terrorism	Upto life imprisonment
67	Publishing/transmitting obscene material in electronic form	***On First Conviction:*** Imprisonment upto 3 years and fine upto 10 lacs. ***On Second/subsequent conviction:*** Imprisonment upto 5 years and fine upto Rs. 10 lacs.
67A	Publishing/transmitting of material containing sexually explicit act, etc in electronic form	***On First Conviction*** - Imprisonment upto 5 years and fine upto Rs. 10 lacs ***On Second or subsequent Conviction*** - Imprisonment upto 7 years and fine upto Rs. 10 lacs.
67B	Publishing material depicting children in sexually explicit act in electronic form	***On First Conviction*** - Imprisonment upto 5 years and fine upto Rs. 10 lacs ***On Second or subsequent Conviction*** - Imprisonment upto 7 years and fine upto Rs. 10 lacs.
68	Non-compliance with Controller's directions	imprisonment upto 3 years or fine upto Rs.2 lacs or both.
69	Failure to assist the agency to extend facilities to intercept, monitor or decrypt as required u/s 69.	Imprisonment upto 7 years & shall also liable to fine.
69A	Failure to comply with CG direction	Imprisonment upto 7 years & shall also liable to fine.
69B	Failure to assist in online access to computer resource	Imprisonment upto 3 years & shall also liable to fine.
70	Securing access to protected system in contravention	Imprisonment upto 10 years & shall also liable to fine.
70B	Failure to provide info called for and comply with direction issued by	Imprisonment upto 1 year or fine upto 1 lac or both.
71	Making any **misrepresentation** to, or suppresses any material fact from Controller or Certifying Authority for obtaining licence or electronic signature certificate	Imprisonment upto 2 years or fine upto 1 lac or both.
72	Breach of confidentiality & privacy	Imprisonment upto 2 years or fine upto 1 lac or both.
72A	Disclosure of info in breach of lawful contract	Imprisonment upto 3 years or fine upto 5 lacs or both.
73	Publishing false electronic certificates	Imprisonment upto 2 years or fine upto 1 lac or both.
74	Publication for fraudulent purpose	Imprisonment upto 2 years or fine upto 1 lac or both.

'Tempering with computer source documents' is a common threat for automated business modules. How ITAA 2008 Address this issue with reference to its section 65? RTP May 2014

Section 65: Tampering with Computer Source Documents:

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with ***imprisonment up to 3 years***, **or** with ***fine*** which ***may extend up to Rs. 2 lacs***, **or** ***with both.***

Explanation: For the purposes of this section, "Computer Source Code" means the listing of programmes, computer commands, Design & layout and Programme analysis of computer resource in any form.

Mr. A has received some info about Mr. B on his cellphone. He knows that this info has been stolen by the sender. He not only retained this info 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 ITAA 2008, he can file an FIR with the police. Advice Mr. B detailing the applicable sections of the Act. Case Study: [May 2013]

It is not clear whether Mr. B wants to file an FIR with police against Mr. A or against the sender who has stolen his info or against 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 sections of ITAA 2008 -

- **Section 66A - 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 info which is grossly offensive or has a threatening character; or

(b) Any info which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal threat, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device;

(c) Any e-mail or e-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 3 years and with fine.***

- **Section 66B - 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 3 years or with fine which may extend to Rs. 1 lac or with both***.

- **Section 66E - Punishment for identity theft -**

Whoever, fraudulently or dishonestly make use of the electronic signature or any other unique identification feature of any person, shall be punished with ***imprisonment*** of either description for a term ***which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1 lac.***

Discuss 'Punishment for Cyber Terrorism' u/s 66 F of ITAA 2008. RTP May 2014

Section 66F: Punishment for cyber terrorism -

(1) **Whoever**,-

(A) ***with intent to*** threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, **or**

(B) ***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.

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

Discuss the 'Power to authorize & collect data or info through any computer resource for Cyber Security' u/s 69B of ITAA 2008. RTP May 2012

Section 69B: ***Power to authorize to monitor and collect traffic data or info through any computer resource for Cyber Security-***

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person-in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or info.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub- section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Write short notes on 'The Indian Computer Emergency Response Team'. Also give the functions to be performed by the team in the areas of Cyber Security?

Section 70 B: The Indian Computer Emergency Response Team :

Sec 70B(1) - The CG shall appoint an agency of the government to be called the Indian Computer Emergency Response Team.

Sec 70B(2) - The CG shall provide the agency with a Director General & such other officers & employees as may be prescribed.

Sec 70B(3) - The salary & allowances and terms & conditions of such officers & employees shall be such as may be prescribed.

Sec 70B(4) - ***The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security***,-

(a) collection, analysis and dissemination of information on cyber incidents

(b) forecast and alerts of cyber security incidents
(c) emergency measures for handling cyber security incidents
(d) coordination of cyber incidents response activities
(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
(f) such other functions relating to cyber security as may be prescribed

Briefly describe the applicability of ITAA for offences or contraventions committed outside India.

Section 75 provides for punishment for commission of any offence or contravention by a person outside India irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Describe the provisions relating to 'Confiscation' u/s 76 of ITAA 2008.

Section 76 provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of contravention of any provision of the Act, rules, regulations or orders made there under.
However, ***Where*** it is established to the satisfaction of Court adjudicating the confiscation that ***the person*** in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto ***is found*** , is ***not responsible for the contravention*** of the provisions of this Act, rules, orders or regulations made there under, ***the court may***, instead of making an order for confiscation of such computer , computer system, floppies, compact disks, tape drives or any other accessories related thereto, ***make such other order*** authorized by this Act, ***against the person contravening the provisions*** of this Act, rules, orders or regulations made there under ***as it may think fit***.

CHAPTER-XII: INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

State the cases specified u/s 79 of ITAA, where the Intermediaries/Network Service Providers are liable (And also where they are not liable) for any third party info, data or communication link made available by them.

Section 79 provides that a Network Service Provider (Intermediary) shall not be liable for any third party information or data made available by him if he proves that the offence was committed without his knowledge or consent.
Explanation - For the purposes of this section -
(a) "*Network Service Provider*" means an **'Intermediary'.**
(b) "*Third Party Information*" means any info dealt with by a network service provider in his capacity as an intermediary.
Section 79: Exemption from liability of Intermediary in certain cases -
Sec 79(1) - Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) & (3), an intermediary shall not be liable for any third party info, data, or communication link hosted by him.
Sec 79(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 info made available by third parties is transmitted or temporarily stored; or
(b) the intermediary does not -
- initiate the transmission,
- select the receiver of the transmission, and
- select or modify the info contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act & also observes such other guidelines as the CG may prescribe in this behalf.
Sec 79(3) - ***The provisions of sub-section (1) shall not apply, if (i.e he will be liable in following cases*****)**
(a) the intermediary has conspired or abetted or aided or induced whether by threat or promise or otherwise in the commission of the unlawful act
(b) upon receiving actual knowledge it fails to immediately remove the material.

CHAPTER-XIIA: EXAMINER OF ELECTRONIC EVIDENCE

Section 79A states that for the purposes of providing expert opinion on electronic form evidence before any court or other authority, the central government may appoint an Examiner of Electronic Evidence.

CHAPTER-XIII: MISCELLANEOUS

Mention the Powers of Police Officers and other officers for Entry & Search.

Section 80 deals with the power of Police Officer and Other Officers to Enter, Search, etc. It prescribes:
Sec 80 (1) - Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of a **Inspector** or any other officer of the CG or a SG authorized by the CG in this behalf, may enter any public place and search & arrest **without warrant** any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.
Explanation**:** For the purposes of this sub-section, the expression "Public Place" includes any public conveyance, any hotel, any shop or other place intended for use by, or accessible to the public.
Sec 80 (2) - Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall,without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.
Sec 80 (3) - The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

Write short notes on "Offences by Companies". **Nov 2008**

Section 85 of ITAA 2008 deals with the offences made by companies. It describes -

Sec 85 (1) - Where a company commits any offence under this Act or any rule thereunder, every person who, at the time of the contravention, was in charge of and was responsible for the conduct of the business of the company shall be guilty of the contravention and shall be liable to be proceeded against & punished accordingly.
However, he shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention.
Sec 85 (2) - Notwithstanding anything contained in sub-section (1) , where a contravention has been committed by a company, and it is proved that the contravention took place with the connivance or consent of or due to any negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty and shall be liable to be proceeded against and punished accordingly.
***Explanation*:** For the purposes of this section, **'Company'** includes a firm or other association of persons; and **'Director'** in relation to a firm means a partner in the **firm.**

Briefly explain the Powers of CG to make rules u/s 87 of Chapter XII of ITAA 2008. May 2008

Section 87 of ITAA deals with the Power of Central Government to make rules, which is described as under -
Sec 87 (1) - ***The CG may***, by notification in the official gazette, ***make rules*** to carry out the provisions of this Act.
Sec 87 (2) - In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely -
1. The conditions for considering reliability of electronic signature or electronic authentication technique;
2. The electronic form in which filing, issue, grant or payment shall be effected u/s 6 (1);
3. The manner & format in which electronic records shall be filed or issued and the method of payment u/s 6 (2);
4. The matters relating to the type of electronic signature, manner & format, in which, it may be affixed u/s 10;
5. The manner of storing & affixing electronic signature creation data u/s 15;
6. The qualifications, experience and terms & conditions of service of Controller, Deputy Controller and Assistant Controllers, other employees u/s 17;
7. The period of validity of licence granted u/s 21(3)(a);
8. The powers & functions of Chairperson of the Cyber Appellate Tribunal u/s 52A;

Sec 87 (3) - Every notification made by the CG u/s 70A(1) and every rule made by it shall be laid, as soon as may be after it is made, before each **House of Parliament**, while it is in session, for a total period of **30 days** which may be comprised in one session or in two or more successive sessions, and **if both houses agree** in making any modification in the regulation, or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect in such modified form or be of no effect, as the case may be.

Write short notes on the Constitution of Cyber Regulations Advisory Committee u/s 88 of ITAA 2008. Nov 2012

Section 88: Cyber Regulation Advisory Committee -
1. The CG shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.
2. The Cyber Regulations Advisory Committee shall consist of a **Chairperson** and such no. of other official & non-official members representing the interests principally affected or having special knowledge of the subject matter as the CG may deem fit
3. The Cyber Regulations Advisory Committee shall advise -
 (a) The CG either generally as regards any rules or for any other purpose connected with this Act;
 (b) The Controller in forming the regulations under this Act
4. There shall be paid to the non-official members of such committee such **traveling & other allowances** as the CG may fix.

Describe the Powers of Controller u/s 89 to make regulations consistent with ITAA 2008. May 2007

1. ***The Controller may***, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the CG, by notification in the official gazette, ***make regulations consistent with this Act*** and the rules made there under to carry out the purposes of this Act.
2. In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely -
 (i) The particulars relating to the maintenance of ***data-base containing the disclosure record of every Certifying Authority***;
 (ii) The Conditions & restrictions subject to which, the Controller may recognise any foreign Certifying Authority u/s 19(1);
 (iii) The terms & conditions, subject to which, a licence may be granted u/s 21(3)(c);
 (iv) Other standards to be observed by a Certifying Authority.
3. Every regulation made under this Act shall be laid, as soon as may be after it is made, before each **House of Parliament**, while it is in session, for a total period of **30 days** which may be comprised in one session or in two or more successive sessions, and **if both houses agree** in making any modification in the regulation, or both Houses agree that the regulation should not be made, the regulation shall thereafter have effect in such modified form or be of no effect, as the case may be.

Describe the Powers of State Government to make rules u/s 90 of ITAA 2008.

1. The SG may, by notification in the official gazette, ***make rules*** to carry out the provisions of this Act.
2. In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely -
 (a) The electronic form in which filing, issue, grant or payment shall be effected u/s 6 (1);
 (b) For matters specified u/s 6(2);
3. Every rule made by the SG under this section, shall be laid, as soon as may be after it is made, before each House of State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.