

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

1. (a) What are the characteristics of a business system?
(b) Explain, in brief, the human resource management system.
2. Define the following terms briefly:
 - (a) Open system
 - (b) Closed system
 - (c) Deterministic System
 - (d) Probabilistic system
 - (e) Transaction Processing System (TPS)
 - (f) Decision Support System (DSS)
 - (g) Executive Information System (EIS).
3. (a) Explain different levels of management activities in management planning and control hierarchy.
(b) Explain various purposes of an Executive Information System (EIS).
4. Explain the System Development Life Cycle.
5. What are the Systems Development Tools? Explain briefly.
6. What do you understand by feasibility study? Explain various types of feasibility studies.
7. Explain the role of IS Auditor with respect to quality control of systems.
8. Write short notes on the following:
 - (i) Locks on Doors with respect to physical access control
 - (ii) Data encryption standard
 - (iii) Hacking
 - (iv) Firewalls.
9. Discuss the role of IS auditor with respect to
 - (a) Physical access controls
 - (b) Environmental controls.
10. What is Black Box testing? Explain briefly.
11. What are the different types of test plans used for software testing?
12. Explain the types of software testing.
13. Explain how review of controls over Network is carried out.

14. Define the following terms:
 - (i) Risk
 - (ii) Threat
 - (iii) Vulnerability
 - (iv) Exposure
 - (v) Malicious Code.
15. What do you understand by the term Risk Assessment? What areas need to be focused for risk assessment?
16. Explain briefly the software and data back-up techniques.
17. (a) Explain audit tools and techniques used for disaster recovery plan.
(b) Describe contents of a disaster recovery and planning document.
18. Give objectives and goals of business continuity planning.
19. (a) What is an ERP?
(b) What are the major features of ERP?
20. What are the steps involved in the implementation of an ERP package?
21. What are the four domains identified under COBIT for high level classification?
22. (a) What do you mean by Software Process Maturity?
(b) Under BS 7799 (Part II), what are the Information Security Management Standards?
23. What are the types of service auditor's reports under SAS 70?
24. What are the various types of Information Security Policies? What are the hierarchical relationships between these policies? Discuss briefly.
25. (a) What are the components of the Security Policy?
(b) What is meant by physical and environmental security?
26. What is meant by SYSTRUST and WEBTRUST? Discuss in brief.
27. (a) What are the duties of a certifying authority under Section 30 of the Information Technology Act 2000?
(b) Define the following terms with reference to section 2 of IT Act, 2000:
 - (i) Digital signature
 - (ii) Electronic form
 - (iii) Key pair
 - (iv) Asymmetric crypto system
 - (v) Adjudicating officer.

28. What are the regulations relating to the appointment and powers of the certifying authorities under Chapter VI, Section 17 to 25 of the IT Act 2000?

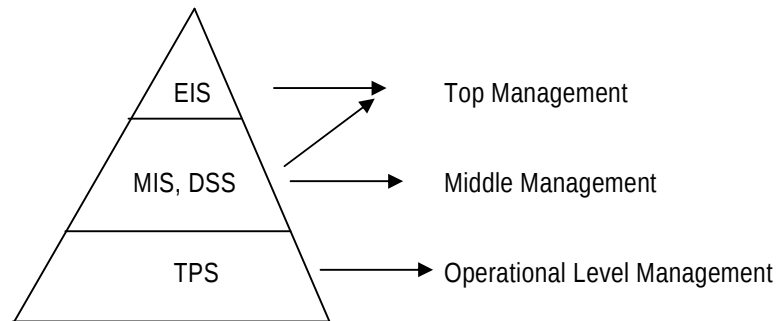
SUGGESTED ANSWERS/HINTS

1. (a) Characteristics of a business system: A business system is an organized grouping of interdependent functioning units or components, linked together according to a plan, to achieve a specific objective. All systems have some common characteristics. These are as follows:
 - (i) All systems work for predetermined objectives and the system is designed and developed accordingly.
 - (ii) In general a system has a number of interrelated and interdependent sub-systems or components. No subsystem can function in isolation, it depends on other sub-systems for its inputs.
 - (iii) If one sub-system or component of a system fails, in most cases the whole system does not work. However, it depends on how the sub-systems are interrelated.
 - (iv) The way a subsystem works with another sub-system is called interaction. The different sub-systems interact with each other to achieve the goal of the system.
 - (v) The work done by individual sub-systems is integrated to achieve the central goal of the system. The goal of individual sub-system is of lower priority than the goal of the entire system.
- (b) Human resource management system: Human resources are the most valuable asset for an organisation. Utilization of these resources in most effective and efficient way is an important function for any enterprise. Human resource management system aims to achieve this goal. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc., helps management for allocating manpower to right activity at the time of need or starting a new project. This system also keeps track of employees' output or efficiency. Administrative functions like keeping track of leave records or handling other related functions are also included in HRM system. An HRM system may have the following modules.
 - Personal administration
 - Recruitment management
 - Travel management
 - Benefit administration
 - Salary administration
 - Promotion management.

An ideal HR development emphasizes on optimal utilization of human resources by introducing a consistent and coherent policy aiming at promoting commitment to the enterprise. The HRM system assists to achieve this goal.

2. (a) Open System: A system that interacts freely with its environment by taking input and returning output is termed as an open system.
- (b) Closed System: A system that does not interact with the environment or does not change with the changes in environment is termed as a closed system.
- (c) Deterministic System: A deterministic system operates in a predictable manner. The interaction among the parts is known with certainty. If one has a description of the systems at a given point in time plus a description of its operation, the next state of the system may be given exactly, without error.
- (d) Probabilistic System: It can be described in terms of probable behaviour, but a certain degree of error is always attached to the prediction of what the system will do.
- (e) Transaction Processing System (TPS): It manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use.
- (f) Decision Support System (DSS): It is a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own, somewhat personalized way. That is, a DSS supports the human decision-making process, rather than providing a means to replace it.
- (g) Executive Information Systems (EIS): It is a tool that provides direct on-line access to relevant information in a useful and navigable format. Relevant information is timely, accurate and actionable information about the aspects of a business that are of particular interest to the senior manager.
3. (a) Different Levels of Management activities: Management at different levels take decisions matching to their position or hierarchy in the organization and different types of information systems are designed and developed for them, i.e. an information system for a departmental manager will be characteristically different from one designed for a corporate manager.

If we consider an organization having a pyramidal management structure with the corporate level managers at the top and operational managers at the bottom we will observe that typical categories of data are manipulated at different levels.



The above figure exhibits data available at different functional areas of an organization for management. At the lowest level that is managed by operational level managers (like supervisor, section in-charge), all types of inputs available from various sources are collected. The routine office work, like maintaining inward register and public interaction are mostly done at this level. However, no decision-making process is carried out at this level.

At the middle level of management the decision making – process starts. Inputs from different internal and external information sources are collected (normally passed from operational level managers) and processed for strategic decisions. Middle level managers who are expected to contribute significantly towards development of the organization are the key personnel to carry out the processing activities of the strategic data. They use various tools of analysis and typical software products to report to the higher level with options and possible effects. This job is very critical and important as well because tactical decisions by the top management are dependent on the information passed from middle management.

(b) Purposes of an EIS: These are stated below:

- (i) The primary purpose of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment. Informed managers can ask better questions and make better decisions.
- (ii) A secondary purpose for an EIS is to allow timely access to information. All of the information contained in an EIS can typically be obtained by a manager through traditional methods. However, the resources and time required to manually compile information in a wide variety of formats, and in response to ever changing and even more specific questions usually inhibit managers from obtaining this information.
- (iii) A third purpose of an EIS is commonly misperceived. An EIS has a powerful ability to direct management attention to specific areas of the organization or specific business problems. Some managers see this as an opportunity to

discipline subordinates. Some subordinates fear the directive nature of the system and spend a great deal of time trying to outfit or discredit it. Neither of these behaviours is appropriate or productive. Rather, managers and subordinates can work together to determine the root causes of issues highlighted by the EIS.

4. System Development Life Cycle Activities:

The system development life cycle method can be thought of as a set of activities that analysts, designers and users carry out to develop and implement an information system.

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

- (i) Preliminary investigation
 - (ii) Requirements analysis or system analysis
 - (iii) Design of system
 - (iv) Development of software
 - (v) System testing
 - (vi) Implementation and maintenance.
- (i) Preliminary investigation: A preliminary investigation is undertaken when users come across a problem or opportunity and submit a formal request for a new systems to the MIS department. This activity consists of three parts: request clarification, feasibility study and request approval. Before any system investigations can be considered, the system request must be examined to determine precisely what the originator wants. Thereafter, the analyst tries to determine whether the system requested is feasible or not. Aspects of technical, economic and operational feasibility of the system are covered in the feasibility study. The third part of the investigation relates to approval of the request. Not all requested systems are desirable or feasible. Based on the observations of the analyst, the management decides which system should be taken up for development.
 - (ii) Requirements analysis or system analysis: If, after studying the result of preliminary investigation, management decides to continue the development process, the needs of the users are studied. Several fact-finding techniques and tools such as questionnaires, interviews, observing decision-maker behaviour and their office environment etc. are used for understanding the requirements. All details are gathered, the analysts study the present system to identify its problems and shortcomings and identify the features, which the new system should include to satisfy the new or changed user application environment.
 - (iii) Design of system: The design of an information system produces the details that state how a system will meet the requirements identified above. The analyst designs various reports / outputs, data entry procedures, inputs, files and database. He also selects file structures and data storage devices. These detailed design

specifications are then passed on to the programming staff so that software development can begin.

- (iv) Acquisition and development of software: After the system design details are resolved, such resources needs as specific type of hardware, software and services are determined. Subsequently, choices are made regarding which products to buy or lease from which vendors. Software developers may install or modify and then install purchased software or they may write new, custom-designed program. The analyst works closely with the programmers if the software is to be developed in-house. During this phase, he analyst also works with users to develop worthwhile documentation for software, including various procedure manuals.
- (v) System testing: Before the information systems can be used, it must be tested. System testing will run according to its specifications and in the way users expect. If it is found satisfactory, it is eventually tested with actual data from the current systems.
- (vi) Implementation and maintenance: After the system is found to be fit, it is implemented with the actual data. Hardware is installed and users are then trained on the new system and eventually work on it is carried out independently. The results of the development efforts are reviewed to ensure that the new system satisfies user requirements. After implementation, the systems is maintained, it is modified to adapt to changing users and business needs so that the system can be useful to the organization as long as possible.

The system development life cycle should be viewed as a continuous interactive process that recycles through each stage for many applications. Thus, even when a system is fully specified, designed, purchased and running, it is continually being enhanced or maintained. Enhancement and maintenance may require returning to one of the earlier stages of system development life cycle.

5. System Development Tools: Tools and Techniques have been developed to improve current information systems and to develop new ones. The major tools used for system development can be grouped into the following four categories based on the systems features each document has:
 - (i) System Components and flows: These tools help the system analysts to document the data flow among the major resources and activities of an information system. System flow charts are typically used to show the flow of data media as they are processed by the hardware devices and manual activities. A data flow diagram uses a few simple symbols to illustrate the flow of data among external entities (such as people or organization etc) processing activities and data storage elements.
 - (ii) User Interface: Designing the interface between end users and the computer system is a major consideration of a system analyst while designing the new system. Layout forms and screens are used to construct the formats and contents

of input / output media and methods. Dialogue flow diagrams analyse the flow of dialogue between computers and people.

- (iii) **Data attributes and relationships:** The data resources in information system are defined, catalogued and designed by this category of tools. A data dictionary catalogs the description of the attributes (characteristics) of all data elements and their relationships to each other as well as to external systems. Entity-relationships diagrams are used to document the number and type of relationship among the entities in a systems. File layout forms document the type, size and names of the data elements in a system. Grid charts help in identifying the use of each type of data element in input / output or storage media of a system.
 - (iv) **Detailed system process:** These tools are used to help the programmer develop detailed procedures and processes required in the design of a computer program. Decision trees and decision tables use a network or tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system.
6. **Feasibility Study:** It refers to the process of evaluating alternative systems through cost / benefit analysis so that the most feasible and desirable system can be selected for development. The feasibility study of a system is undertaken from three angles: technical, economic and operational feasibility.

Technical feasibility: It is concerned with hardware and software. The technical issues usually raised during the feasibility stage of investigation include the following:

- (i) Does the necessary technology exist to do what is suggested (and can it be acquired)?
- (ii) Does the proposed equipment have the technical capacity to hold the data required to use the new system?
- (iii) Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users?
- (iv) Can the system be expanded if developed?
- (v) Are there technical guarantees of accuracy, reliability, ease of access and data security?

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

- (i) The cost of conducting full systems investigation.
- (ii) The cost of hardware and software for the class of applications being considered.
- (iii) The benefits in the form of reduced costs or fewer costly errors.
- (iv) The cost if nothing changes.

Operational feasibility: It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility.

Some of the questions which help in testing the operational feasibility of a project are:

- ◆ Is there sufficient support for the system from management? From users? If the current system is well liked and used to the extent that persons will not be able to see reasons for a change, there may be resistance.
- ◆ Are current business methods acceptable to users? If they are not, users may welcome a change that will bring about a more operational and useful system.
- ◆ Have the users been involved in planning and development of the project? Early involvement reduces the chance of resistance to the system and changes in general and increases the likelihood of successful projects.
- ◆ Will the proposed system cause harm? Will it produce poorer results in any aspects or areas? Will loss of control result in any areas? Will accessibility of information be lost? Will individual performance be poorer after implementation than before? Will performance be affected in an undesirable way? Will the system slow performance in any areas?

Schedule Feasibility: It involves the design team's estimation how long it will take a new or revised system to become operational and communicating this information to the steering committee.

Legal Feasibility: Legal feasibility is largely concerned with whether there will be any conflict between a newly proposed system and the organisation's legal obligations. For example, a revised system should comply with all applicable federal and state statutes about financial reporting requirements, as well as the company's contractual obligations.

7. IS Auditor's Role: In case, the auditor intends to carry out detailed reviews of, for example, logical design, it will probably be necessary either to employ expert assistance, or to undertake training in the particular technical skills required.

The following are the general questions that the IS Auditor needs to consider for quality control:

- (a) does system design follow a defined and acceptable standard?
- (b) are completed designs discussed and agreed with the users?
- (c) does the project's quality assurance procedures ensure that project documentation is reviewed against the organisation's technical standards and policies, and the user requirements specification.
- (d) do quality reviews follow a defined and acceptable standard?
- (e) are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;
- (f) are auditors / security staff invited to comment on the internal control aspects of system designs and development specifications?

- (g) are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analysed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
 - (h) are defects uncovered during quality reviews always corrected?
 - (i) does the production of development specifications also include the production of relevant acceptance criteria?
 - (j) has a configuration manager been appointed? Has the configuration management role been adequately defined?
 - (k) are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?
 - (l) has sufficient IT been provided to assist with the configuration management task?
 - (m) are effective procedures in place for recording, analyzing and reporting failures uncovered during testing?
 - (n) are effective change management procedures in place to control changes to configuration items?
 - (o) has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery?
 - (p) has a system installation plan been developed and quality reviewed?
 - (q) has an acceptance testing plan been drawn up? Is it to an acceptable standard? Does it cover all aspects of the user requirements specification?
 - (r) does the acceptance test plan clearly allocate roles and responsibilities for undertaking and reviewing the results of acceptance testing?
 - (s) has the acceptance test plan been discussed with, and signed off by the prospective system owner?
 - (t) is the system development environment regularly backed up with copies of backed up configuration item held securely at a remote location?
 - (u) has the development environment been recovered from backup media?
 - (v) are contingency plans commensurate with the criticality of the project.
 - (w) do regular project board meetings take place to review project progress against budget and deadline?
 - (x) is the Business Case regularly updated to ensure that the project remains viable?
8. (i) Locks on Doors: Different types of locks on doors for physical security are discussed below:

Cipher Locks (combination Door Locks): The Cipher Lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit

number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.

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

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

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

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

- (ii) Data Encryption Standard (DES): It is a Cipher (a method for encrypting information) selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. It is a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) 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 ('0's or '1's) 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, i.e. there is an odd number of "1" in each 8-bits byte.

- (iii) Hacking: It is an act of penetrating computer systems to gain knowledge about the system and how it works. Technically, a hacker is someone who is enthusiastic about computer programming and all things relating to the technical workings of a computer.

Crackers 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 crackers 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.

There are many ways in which a hacker can hack. These are:

- ◆ Net BIOS
- ◆ ICMP Ping
- ◆ FTP
- ◆ rpc. statd
- ◆ HTTP.

- (iv) Firewalls: A firewall is a collection of components (Computers, routers and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs).

There are four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the system and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

9. (a) Role of IS Auditor in Physical Access Controls: Auditing Physical Access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:
- (i) Risk Assessment: The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
 - (ii) Controls Assessment: The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
 - (iii) Planning for review of physical access controls: It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.
 - (iv) Testing of Controls: The auditor should review physical access controls to satisfy for their effectiveness. This involves:
 - ◆ Tour of organisational facilities including outsourced and offsite facilities.
 - ◆ Physical inventory of computing equipment and supporting infrastructure.

- ◆ Interviewing personnel can also provide information on the awareness and knowledge of procedures.
 - ◆ Observation of safeguards and physical access procedures. This would also include inspection of:
 - (i) Core computing facilities.
 - (ii) Computer storage rooms.
 - (iii) Communication closets.
 - (iv) Backup and off site facilities.
 - (v) Printer rooms.
 - (vi) Disposal yards and bins.
 - (vii) Inventory of supplies and consumables.
 - ◆ Review of physical access procedures including user registration and authorization, authorization for special access, logging, review, supervision etc. Employee termination procedures should provide withdrawal of rights such as retrieval of physical devices like smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organization.
 - ◆ Examination of physical access logs and reports. This includes examination of incident reporting logs and problem resolution reports.
- (b) Role of Auditor in Environment Controls: The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and environmental controls. Audit of environment controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but that the overall controls assure safeguarding the business against environmental risks. Some of the critical audit considerations that an IS auditor should take into account while conducting his audit are given below:

Audit Planning and Assessment: As part of risk assessment:

- ◆ The risk profile should include the different kinds of environmental risks that the organisation is exposed to. These should comprise both natural and man-made threats. The profile should be periodically reviewed to ensure updation with newer risk that may arise.
- ◆ The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones and are in place.
- ◆ The security policy of the organization should be reviewed to access policies and procedures that safeguard the organization against environmental risks.

- ◆ Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
- ◆ The IS Auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling, and evacuation procedures to determine if adequate incident reporting procedures exist.
- ◆ Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.

Audit of Technical Controls: Audit of environmental controls requires the IS Auditor to conduct physical inspections and observe practices. He must verify:

- ◆ The IPF and the construction with regard to the type of materials used for construction.
- ◆ The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs.
- ◆ The location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers.
- ◆ Emergency procedures, evacuation plans and making of fire exists. If necessary, the IS Auditor may also use a mock drill to test the preparedness with respect to disaster.
- ◆ Documents for compliance with legal and regulatory requirements with regard to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors / auditors.
- ◆ Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power.
- ◆ Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionisers etc.
- ◆ Compliant logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
- ◆ Activities in the IPF. Identify undesired activities such as smoking, consumption of eatables etc.

10. **Black Box Testing:** Black Box Testing attempts to derive sets of inputs that will fully exercise all the functional requirements of a system. It is not an alternative to white box

testing. This type of testing attempts to find errors in the following categories:

- (1) Incorrect or missing functions;
- (2) Interface errors;
- (3) errors in data structures or external database access;
- (4) performance errors, and
- (5) initialisation and termination errors.

Tests are designed to answer the following questions:

- ◆ How is the function's validity tested?
- ◆ What classes of input will make good test cases?
- ◆ Is the system particularly sensitive to certain input values?
- ◆ How are the boundaries of a data class isolated?
- ◆ What data rates and data volume can the system tolerate?
- ◆ What effect will specific combinations of data have on system operation?

Various methods to conduct black box testing are discussed briefly below:

Equivalence partitioning: This method divides the input domain of a program into classes of data from which test cases can be derived. Equivalence partitioning strives to define a test case that uncovers classes of errors and thereby reduces the number of test cases needed. It is based on an evaluation of equivalence classes for an input condition. An equivalence class represents a set of valid or invalid states for input conditions.

Equivalence classes may be defined according to the following guidelines:

- (1) If an input condition specifies a range, one valid and two invalid equivalence classes are defined.
- (2) If an input condition requires a specific value, then one valid and two invalid equivalence classes are defined.
- (3) If an input condition specifies a member of a set, then one valid and one invalid equivalence class are defined.
- (4) If an input condition is Boolean, then one valid and one invalid equivalence class are defined.

Boundary Value Analysis (BVA): This method leads to a selection of test classes that exercise boundary values. It complements equivalence partitioning since it selects test cases at the edges of a class. Rather than focusing on input conditions solely, BVA derives test cases from the output domain also. BVA guidelines include:

- (1) For input ranges bounded by a and b, test cases should include values a and b and just above and just below a and b respectively.

- (2) If an input condition specifies a number of values, test cases should be developed to exercise the minimum and maximum numbers and values just above and below these limits.
- (3) Apply guidelines 1 and 2 to the output.
- (4) If internal data structures have prescribed boundaries, a test case should be designed to exercise the data structure at its boundary.

Cause-Effect Graphing Techniques: Cause – effect graphing is a technique that provides a concise representation of logical conditions and corresponding actions. There are four steps:

- (1) Causes (input conditions) and effects (actions) are listed for a module and an identifier is assigned to each.
- (2) A cause-effect graph is developed.
- (3) The graph is converted to a decision table.
- (4) Decision table rules are converted to test cases.

11. Test Plan: The test strategy identifies multiple test levels, which are going to be performed for the project. Activities at each level must be planned well in advance and it has to be formally documented. Based on the individual plans only, the individual test levels are carried out. Test Plans may be of different types:

- ◆ Unit test plan
- ◆ Integration test plan
- ◆ System test plan
- ◆ Acceptance test plan.

- (i) Unit Test Plan (UTP): The unit test plan is the overall plan to carry out the unit test activities. The lead tester prepares it and it is distributed to the individual testers, which contains the following sections.

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

Sequence of Testing: The sequences of test activities that are to be carried out in this phase are to be listed in this section. This includes whether to execute positive test cases first or negative test cases first, to execute test cases based on the priority, to execute test cases based on test groups etc. Positive test cases prove that the system performs what is supposed to do; negative test cases prove that the

system does not perform what is not supposed to do. Testing the screens, files, database etc. are to be given in proper sequence.

- ◆ Basic functionality of units: How the independent functionalities of the units are tested which excludes any communication between the unit and other units. The interface part is out of scope of this test level. Apart from the above sections, the following sections are addressed, very specific to unit testing.
- ◆ Unit testing tools
- ◆ Priority of program units
- ◆ Naming convention for test cases
- ◆ Status reporting mechanism
- ◆ Regression test approach.

- (ii) Integration test plan: The integration test plan is the overall plan for carrying out the activities in the integration test level, which contains the following sections.

What is to be tested? This section clearly specifies the kinds of interfaces which fall under the scope of testing viz., internal and external interfaces. There is no need to go deep in terms of technical details but the general approach i.e. how the interfaces are triggered is explained.

Sequence of Integration: When there are multiple modules present in an application, the sequence in which they are to be integrated will be specified in this section. In this, the dependencies between the modules play a vital role. If a unit B has to be executed, it may need the data that is fed by unit A and Unit X. In this case, the units A and X have to be integrated and then using that data, the unit B has to be tested. This has to be stated to the whole set of units in the program. Given this correctly, the testing activities will lead to the product, slowly building the product, unit by unit and then integrating them.

- (iii) System Test Plan (STP): The system test plan is the overall plan carrying out the system test level activities. In the system test, apart from testing the functional aspects of the system, there are some special testing activities carried out, such as stress testing etc. The following are the section normally present in system test plan.

What is to be tested? This section of defines the scope of system testing, very specific to the project. Normally, the system testing is based on the requirements. All requirements are to be verified in the scope of system testing. This covers the functionality of the product. Apart from this what special testing is performed are also stated here.

Functional Groups and the sequence: The requirements can be grouped in terms of the functionality. Based on this, there may also be priorities among the functional groups. For the product being tested, areas are to be mentioned and the suggested sequences of testing of these areas, based on the priorities are to be described.

- (iv) Acceptance Test Plan (ATP): The client at their place performs the acceptance testing. It will be very similar to the system test performed by the software development unit. Since the client is the one who decides the format and testing methods as part of acceptance testing, there is no specific clue on the way they will carry out the testing. However, but it will not differ much from the system testing. Since this is just one level of testing done by the client for the overall product, it may include test cases including the unit and integration test level details.
12. Types of Software Testing: There are two types of software testing. They are:
- (i) Static Testing: The verification activities fall into the category of static testing. During static, you have a checklist to check whether the work you are doing is going as per the set standards of the organization. These standards can be for coding, integrating and deployment. Reviews, inspections and walkthroughs are static testing methodologies.
 - (ii) Dynamic Testing: Dynamic testing involves working with the software, giving input values and checking if the output is as expected. These are the validation activities. Unit tests, integration tests, system tests and acceptance tests are few of the dynamic testing methodologies.
13. Review of control over Network: The review of controls over LANs is done to ensure that standards are in place for designing and selecting a LAN architecture and for ensuring that the costs of procuring and operating the LAN do not exceed the benefits.
- 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:
- ◆ LAN topology and network design.
 - ◆ Significant LAN components (such as servers and modems)
 - ◆ Network topology (including internal LAN configuration) as well as interconnections to other LANs, WANs or public networks).
 - ◆ LAN uses, including significant traffic types and main applications used over the network.
 - ◆ LAN administrator.
 - ◆ Significant groups of LAN users.
- In addition, the reviewer should gain an understanding of the following:
- ◆ Functions performed by the LAN administrator.
 - ◆ The company's division or department procedures and standards relating to network design support, naming conventions and data security.
 - ◆ LAN transmission media and techniques, including bridges, routers and gateways.

Understanding the above information should enable the reviewer to make an assessment of the significant threats to the LAN, together with the potential impact and probability of occurrence of each threat.

Physical controls should protect LAN hardware and access points to the LAN by limiting access to those individuals authorized by management. Company data stored on a file server is easier to damage or steal than when on a mainframe and should be physically protected. The reviewer should review the following:

LAN hardware devices, particularly the file server and documentation, should be located in a secure facility and restricted to the LAN administrator. The wiring closet and cabling should be secure.

Keys to the LAN file server facility should be controlled to prevent or minimise the risk of unauthorised access.

LAN file server housing should be locked or otherwise secured to prevent removal of boards, chips and the computer itself.

14. (i) Risk: It is the probability that an event or action will adversely effect the organization. Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by:
 - (a) Widespread use of technology.
 - (b) Interconnectivity of systems.
 - (c) Elimination of distance, time and space as constraints.
 - (d) Unevenness of technological changes.
 - (e) Devolution of management and control.
 - (f) Attractiveness of conducting unconventional electronic attacks against organisations.
 - (g) External factors such as legislative, legal and regulatory requirements or technological developments.
- (ii) Threats: It is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services.
- (iii) Vulnerability: It is the weaknesses in the system safeguards that exposes the system to threats. It may be weaknesses in an information system, cryptographic system (security systems) or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For

example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records.

- (iv) Exposure: It is the extent of loss the organization has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run, for example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources.
 - (v) Malicious code: It is a code such as viruses and worms which freely access the unprotected networks which may affect organisational and business networks that use these unprotected networks.
15. Risk Assessment: A risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters. Through risk analysis, it is possible to identify, assess and then mitigate the risk.

Risk Assessment is a critical step in disaster and business continuity planning. Risk Assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan.

The areas to be focused upon are:

- (a) Prioritisation: All applications are inventoried and critical ones identified. Each of the critical application is reviewed to assess its impact on the organisation, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
- (b) 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 based on its present value, future changes should not be ignored.
- (c) Assessing their impact on the organisation: Business continuity planning should not concentrate only on business disruption but should also take into account other organizational functions which may be affected. The areas to be considered include:
 - ◆ Legal liabilities
 - ◆ Interruptions of customer services.
 - ◆ Possible losses
 - ◆ Likelihood of fraud and recovery procedures.
- (d) Determining recovery time-frame: Critical recovery time period is the period of time in which business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature of operations. It is

essential to involve the end users in the identification of critical functions and critical recovery time period.

- (e) **Assess Insurance Coverage:** The information system insurance policy should be a multiperil policy, designed to provide various types of coverage. Depending on the individual organisation and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:
 - (i) **Hardware and facilities:** The equipment should be covered adequately. Provision should be made for the replacement of all equipment 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 clients. The loss of profit caused by the damaged computer media should be covered.
 - (v) **Valuable paper and records:** The actual cost of valuable papers and records stored in the insured premises should be covered.
 - (vi) **Errors and omissions:** This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmes and other information system personnel.
 - (vii) **Fidelity coverage:** This coverage is for acts of employees more so in the 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 / premises should be covered.
 - (f) **Identification of exposures and implications:** It is not possible to accurately predict as to when and how a disaster would occur. So it is necessary to estimate the probability and frequency of disaster.
 - (g) **Development of recovery plan:** The plan should be designed to provide for recovery from total destruction of a site.
16. **Software and Data Back-up Techniques:** When the back-ups are taken of the system and data together, they are called total system's back-up. Systems back-up may be a full back-up, an incremental back-up or a differential back-up.
- (i) **Full Back-up:** This is the simplest form of back-up. With a full back-up system, every back-up generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. When it comes to restoring data,

this type of backup is the simplest to use because a single restore session is needed for restoring all back-up files.

- (ii) **Differential Back-up:** A differential backup generation contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup.

Comparing with full back-up, differential back up is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

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

- (iii) **Incremental Backup:** In an incremental backup generation only the files that have changed since the last full backup / differential back up / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.
 - (iv) **Mirror backup:** It is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.
17. (a) **Audit Tools and Techniques:** The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as under:
- (i) **Automated Tools:** Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software etc.
 - (ii) **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
 - (iii) **Disaster and security checklists:** A checklist can be used against which the systems can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
 - (iv) **Penetration Testing:** Penetration testing can be used to locate vulnerabilities.

(b) Disaster Recovery Procedural Plan Document: The disaster recovery and planning document may include the following areas:

- ◆ The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- ◆ Emergency procedures, which describe the action to be taken following an incident which jeopardizes business operations and / or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- ◆ Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- ◆ Resumption procedures, which describe the actions to be taken to return to normal business operations.
- ◆ A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- ◆ Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- ◆ The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternative should be nominated as required.
- ◆ Contingency plan document distribution list.
- ◆ Detailed description of the purpose and scope of the plan.
- ◆ Contingency plan testing and recovery procedure.
- ◆ List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- ◆ Check-list for inventory taking and updating the contingency plan on a regular basis.
- ◆ List of phone numbers of employees in the event of an emergency.
- ◆ Emergency phone list for fire, police, hardware, software suppliers, customers, back-up location, etc.
- ◆ Medical procedure to be followed in case of injury.
- ◆ Backup location contractual agreement, correspondences.
- ◆ Insurance papers and claim forms.
- ◆ Primary computers Centre hardware, software, peripheral equipment and software configuration.

- ◆ Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- ◆ Alternate manual procedures to be followed such as preparation of invoices.
- ◆ Names of employees trained for emergency situation, first aid and life saving techniques.
- ◆ Details of airlines, hotels and transport arrangements.

18. **Objectives and Goals of Business Continuity Planning:** The primary objective of a business continuity plan is to enable an organisation to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

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

Therefore, the goals of the business continuity plan should be to:

- (i) Identify weaknesses and implement a disaster prevention program;
- (ii) Minimise the duration of a serious disruption to business operations;
- (iii) facilitate effective coordination of recovery tasks;
- (iv) reduce the complexity of the recovery effort.

19. (a) **ERP – Definition:** “An Enterprise resource planning system is a fully integrated business management system covering functional areas of an enterprise like logistics, production, finance, accounting and human resources”.

It organizes and integrates operation processes and information flows to make optimum use of resources such as men, material, money and machine.

“Enterprise resource planning promises one database, one application, and one user interface for the entire enterprise, where once disparate systems ruled manufacturing, distribution, finance and sales.”

(b) Major features of ERP:

- ◆ ERP provides multi-platform, multi-mode manufacturing, multi-currency, multi-lingual facilities.
- ◆ It supports strategic and business planning activities, operational planning and execution activities, creation of materials and resources. All these functions are effectively integrated for flow and update of informations immediately upon entry of any information.
- ◆ Has end to end supply chain management to optimize the overall demand and supply data.
- ◆ ERP facilitates company-wide integrated information system covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory accounts, human resources, purchases etc.
- ◆ ERP performs core activities and increases customers service, thereby augmenting the corporate image.
- ◆ ERP bridges the information gap across organisations.
- ◆ ERP provides complete integration of systems not only across departments but also across companies under the same management.
- ◆ ERP is the solution for better project management.
- ◆ ERP allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Electronic Data Interchange (EDI), Internet, Intranet, Video Conferencing, E-commerce etc.
- ◆ ERP eliminates most business problems like materials shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
- ◆ ERP provides intelligent business tools like decision support system, Executive Information System, Data mining and easy working systems to enable better decisions.

20. Steps of ERP Implementation:

- (i) Identifying the needs for implementing an ERP package.
- (ii) Evaluating the “As Is” situation of the business i.e. to understand the strength and weakness prevailing under the existing circumstances.
- (iii) Deciding the ‘would be’ situation for the business i.e. the changes expected after the implementation of ERP.
- (iv) Re-engineering the Business Process to achieve the desired results in the existing processes.
- (v) Evaluating the various available ERP packages to assess suitability.
- (vi) Finalising of the most suitable ERP package for implementation.

- (vii) Installing the required hardware and networks for the selected ERP package.
- (viii) Finalising the implementation consultants who will assist in implementation.
- (ix) Implementing the ERP package.

21. Domains of COBIT:

Four broad domains of COBIT are stated below:

- (i) Planning and organization.
- (ii) Acquisition and implementation.
- (iii) Delivery and support.
- (iv) Monitoring.
- (i) Planning and organization: This domain covers strategy and tactics and concerns the identification of the way. It can best contribute to the achievement of the business objectives.

The following table lists the high level control objectives for the planning and organization domain:

Entire top and middle tiers of COBIT

Plan and Organise

P 01	Define a strategic IT Plan and direction
P 02	Define the Information Architecture
P 03	Determine Technological Direction
P 04	Define the IT Processes, Organisation and Relationship
P 05	Manage the IT investment
P 06	Communicate Management Aims and Direction
P 07	Manage IT Human Resources
P 08	Manage Quality
P 09	Assess and Manage IT Risks
P 10	Manage Projects
P 11	Manage Quality

- (ii) Acquisition and Implementation: To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

The following table lists the high level control objectives for the Acquisition and Implementation domain:

Entire top and middle tiers of COBIT

Acquire and Implement

A 11	Identify Automated Solutions
A 12	Acquire and Maintain Application Software
A 13	Acquire and Maintain Technology Infrastructure
A 14	Enable Operation and Use
A 15	Procure IT Resources
A 16	Manage Changes
A 17	Install and Accredite Solutions and Changes.

- (iii) Delivery and support: This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.

The following table lists the high level control objectives for the delivery and support domain:

Entire top and middle tiers of COBIT

Deliver and Support

DS 1	Define and Manage service levels
DS 2	Manage Third-party services
DS 3	Manage performance and capacity
DS 4	Ensure continuous service
DS 5	Ensure systems security
DS 6	Identify and allocate costs
DS 7	Educate and train users
DS 8	Manage service desk and incidents
DS 9	Manage the configuration
DS 10	Manage problems
DS 11	Manage data
DS 12	Manage the physical environment
DS 13	Manage operations.

- (iv) Monitoring: All it processes need to be regularly assessed overtime for their quality and compliance with control requirements. This domain thus addresses

management's oversight of the organisations control process and independent assurance provided by internal and external audit or obtained from alternative sources.

The following table lists the high level control objectives for the monitoring domain:

Entire top and middle tiers of COBIT

Monitor and Evaluate

ME 1	Monitor and Evaluate IT Processes
ME 2	Monitor and Evaluate Internal Control
ME 3	Ensure Regulatory Compliance
ME 4	Provide IT Governance.

22. (a) **Software Process Maturity:** This is the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organisation's software process and the consistency with which it is applied in project throughout the organization. As a software organization gains in software process maturity it institutionalizes its software process via policies, standards and organisational structures. Institutionalisation entails building an infrastructure and a corporate culture that supports the methods, practices and procedures of the business so that they endure after those who originally defined them have gone.

- (b) **ISO 27001 – (BS 7799 : Part II) – Information Security Management Standard:**

The requirements of information security system as described by standard are stated below. An organization must take a clear view on these issues before trying to implement an Information Security Management Systems (ISMS).

General: Organisation shall establish and maintain documented ISMS addressing assets to be protected, organisations approach to risk management, control objectives and control, and degree of assurance required.

Establishing Management Framework: This would include:

- ◆ Define Information Security Policy;
- ◆ Define scope of ISMS including functional, assets, technical and locational boundaries;
- ◆ Make appropriate risk assessment;
- ◆ Identify areas of risk to be managed and degree of assurance required;
- ◆ Select appropriate controls;
- ◆ Prepare statement of Applicability.

Implementation: Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.

Documentation: The documentation shall consist of evidence of action undertaken under establishment of the following:

- ◆ Management control.
- ◆ Management framework summary, security policy, control objective and implemented control given in prepare statement of applicability.
- ◆ Procedure adopted to implement control under implementation clause.
- ◆ ISMS management procedure.
- ◆ Document Control: The issue focused under this clause would be:
 - ◆ Ready availability
 - ◆ Periodic review
 - ◆ Maintain version control
 - ◆ Withdrawal when obsolete
 - ◆ Preservation for legal purpose.
- ◆ Records: The issues involved in record maintenance are as follows:
 - ◆ Maintain to evidence compliance to Part 2' of BS 7799;
 - ◆ Procedure for identifying, maintaining, retaining and disposing of such evidence;
 - ◆ Records to be legible, identifiable and traceable to activity involved;
 - ◆ Storage to augment retrieval and protection against damage.

23. Service Auditor's Report: The most effective ways a service organization can communicate information about its controls is through a service Auditor's Report.

There are two types of Service Auditor's Report:

- (1) Type I: A type I report describes the service organisations description of controls at a specific point in time (e.g. June 30, 2003). A type II report not only includes the service organization description of controls, but also includes detailed testing of the service organisation's controls over a minimum six month period (e.g. January 1, 2003 to June 30, 2003). The contents of each type of report are described in the following table:

S. No.	Report Contents	Type I Report	Type II Report
1.	Independent service auditor's report (i.e. opinion)	Included	Included
2.	Service organisation's description of controls	Included	Included
3.	Information provided by the independent service auditor; includes a description of the service	Optional	Included

	auditor's tests of operating effectiveness and the results of those tests.		
4.	Other information provided by the service organization (e.g. glossary of terms)	Optional	Optional

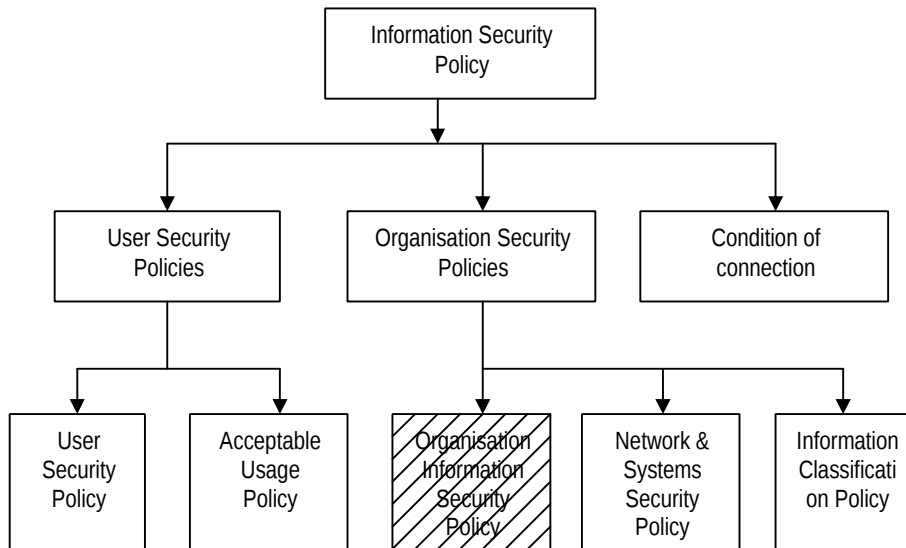
- (2) Type II : In a Type I report, the service auditor will express an opinion on (1) whether the service organisation's description of its controls presents fairly, in all material respects, the relevant aspects of the service organisations controls that had been placed in operation as of a specific date and (2) whether the controls were suitably designed to achieve specified control objectives.

In a type II report, the service auditor will express an opinion on the same items noted above in a type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

24. Types of Information Security Policies and their Hierarchy:

- ◆ Information Security Policy: This policy provides a definition of Information Security, its overall objective and the importance applies to all users.
- ◆ User Security Policy: This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for users, line managers and system owners.
- ◆ Acceptance Usage Policy: This sets out the policy for acceptance use of e-mail and internet services.
- ◆ Organisational Information Security Policy: This policy sets out the Group Policy for the security of its information assets and the Information Technology (IT) Systems processing this information.
- ◆ Network and System Security Policy: This policy sets out detailed policy for system and network security and applies to IT department users.
- ◆ Information classification policy: This policy sets out the policy for the classification of information.
- ◆ Conditions of connection: This policy sets out the group policy for connecting to their network. It applies to all organisations connecting to the group, and relates to the conditions that apply to different supplies systems.

The hierarchy of Information Security Policies



25. (a) Components of the Security Policy: A good security policy should clearly state the following:
- ◆ Purpose and scope of the document and the intended audience.
 - ◆ The security infrastructure.
 - ◆ Security policy document maintenance and compliance requirements.
 - ◆ Incident response mechanism and incident reporting.
 - ◆ Security organization structure.
 - ◆ Inventory and classification of assets.
 - ◆ Description of technologies and computing structure.
 - ◆ Physical and environmental security.
 - ◆ Identify management and access control.
 - ◆ IT operations management.
 - ◆ IT communications.
 - ◆ System development and maintenance controls.
 - ◆ Business continuity planning.
 - ◆ Legal compliances.
 - ◆ Monitoring and Auditing Requirements.

- ◆ Underlying technical policy.

(b) Physical and Environmental Security:

- ◆ Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
- ◆ The IT infrastructure must be physically protected.
- ◆ Access to secure areas must remain limited to authorized staff only.
- ◆ Confidential and sensitive information and valuable asserts must always be securely locked away when not in use.
- ◆ Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to systems.
- ◆ Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities.
- ◆ Wherever practical, premises housing computer equipment and data should be located away from and protected against threats of deliberate or accidental damage such as fire and natural disaster.
- ◆ The location of the equipment room (s) must not be obvious. It should practically be located away and protected against threats of unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

26. SYSTRUST and WEBTRUST: Systrust and Webtrust 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 organisation. System related to e-commerce. Only Certified Public Accountants (CPAs) may provide the assurance services of trust services that result in the expression of a trust services, webtrust, or systrust opinion and in order to issue systrust or webtrust reports, CPA firms must be licensed by the AICPA.

The following principles and related criteria have been developed by the AICPA / CICA for use by practitioners in the performance of Trust services engagements such as systrust and webtrust.

- ◆ Security: The system is protected against unauthorized access (both physical and logical).
- ◆ Availability: The system is available for operation and use as committed or agreed.
- ◆ Processing integrity: System processing is complete, accurate, timely and authorized.
- ◆ On-line privacy: Personal Information obtained as a result of e-commerce is collected, used, disclosed and retained as committed or agreed.

- ◆ Confidentiality: Information designated as confidential is protected as committed or agreed.

Each of these principles and criteria are organized and presented in four broad areas:

- ◆ Policies: The entity has defined and documented its policies relevant to the particular principle.
- ◆ Communications: The entity has communicated its defined policies to authorized users.
- ◆ Procedures: The entity uses procedures to achieve its objectives in accordance with its defined policies.
- ◆ Monitoring: The entity monitors the system and takes action to maintain compliance with its defined policies.

27. (a) Duties of Certifying Authorities {Section 30}:

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

- (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 digital signatures are assured and
- (d) Observe such other standards as may be specified by regulations.
- (b) (i) Digital Signature: It is a authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3:
- (ii) Electronic form: It is reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.
- (iii) Key Pair: It is an asymmetric cryptosystem, 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.
- (iv) Asymmetric crypto system: It is a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.
- (v) Adjudicating Officer: It means an adjudicating Officer appointed under sub-section (1) of section 46.

28. Regulation of Certifying Authorities [Chapter VI – Section 17–25]:

Chapter VI contains detailed provisions relating to the appointment and powers of the Controller and Certifying Authorities.

Section 17 provides for the appointment of Controller and other officers to regulates the Certifying Authorities.

Section 18 lays down the functions which the controller may perform in respect of activities of Certifying Authorities.

Section 19 provides for the power of the Controller with the previous approval of the Central Government to grant recognition to foreign certifying Authorities subject to such conditions and restrictions as may be imposed by regulations.

Section 20 This Section provides that the controller shall be acting as repository of all Digital Signature Certificates issued under the Act. He shall also adhere to certain security procedure to ensure secrecy and privacy of the digital signatures and also to satisfy such other standards as may be prescribed by the Central Government. He shall maintain a computerized database of all public keys in such a manner that they are available to the general public.

Section 21 This section provides that a license to be issued to a certifying authority to issue digital signature certificates by the controller shall be in such form and shall be accompanied with such fees and other documents as may be prescribed by the Central Government. Further, the Controller after considering the application may either grant the licence or reject the application after giving reasonable opportunity of being heard.

Section 22 This Section provides that the application for license shall be accompanied by a certification practice statement and statement including the procedures with respect to identification of the applicant. It shall be future accompanied by a fee not exceeding Rs. 25,000 and other documents as may be prescribed by the Central Government.

Section 23 provides that the application for renewal of a license 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 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.

Section 25 provides that the controller may revoke a licence 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 thereunder.