PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Information Systems Concepts

1. (a) Identify and justify the need for an information system that is designed to meet the special business needs of the strategic level of management in an organization.

   (b) Briefly describe the executive roles at the strategic level of management.

2. As a member of the system development team, explain the process of decomposition of an organization into various functional blocks to comprehend the information processing system with the help of an example.

Software Development Life Cycle Methodology

3. As an internal IS Auditor of an enterprise which is undergoing the phase of system acquisition, how will you prepare the checklists for the following:

   (a) Evaluation and validation of the software package to be acquired,

   (b) The support service to be given by the vendor, and

   (c) Evaluation of the Software License Agreement (SLA).

4. An organization is in the stage of systems development to implement an enterprise wide information system, where the following conditions exist:

   - End users are not aware of the information needs.
   - The new system is mission critical and there is a hasty need.
   - The business risks associated in implementing the wrong system are high.

   Read the above case carefully and answer the following with proper justification/s:

   (a) Identify the system development approach and the steps to be followed in the above stated conditions.

   (b) State the reasons for choosing the particular approach for system development.

   (c) Identify the risks, when end-users are involved in the system development process.

Control Objectives

5. Categorize the controls given below from an Auditor's perspective and state the reasons:

   (a) The user ID of an employee, who initiates a transaction, is recorded in the database.

   (b) Hash totals are calculated both at the sender and receiver end of the data transmission network.

   (c) Data backup procedures are scheduled for every hour on the customer sales records of the enterprise database.

(d) After three attempts of login with wrong password the account is locked for 4 (four) hours.

(e) The employees, authorized to enter the server room, are given embedded chip-based ID-card.

6. The table, given below contains the exposures or vulnerabilities. As an IS Auditor, identify the control type and the control technique to be implemented to mitigate the risk.

S. No.	Exposure
(a)	Records or files assigned to a particular user being modified by another user.
(b)	Anybody can enter the server room.
(c)	To change the contents of the web pages, published on a company's server.
(d)	Failure of hard disks in the database storage system due to spikes in the electrical supply and heating.
(e)	The system development projects/tasks consume excessive resources and unauthorized system changes are recorded.

7. (a) Briefly state the need to install a 'Fire Suppression System' in an information processing facility and the various installation techniques.

(b) Discuss the various environmental control techniques that can be implemented to prevent the unauthorized access for critical IT infrastructures like server room, storage network devices, and switch/router installations.

8. "A financial institute needs to authenticate its electronic credentials by ensuring its PKI policies and controls". Comment on the statement.

9. The validity of the output generated from application software ultimately depends on the user, who is responsible for data submission and correction of errors. Briefly discuss the various user controls and error correction techniques to be followed.

10. As a member of the system implementation and quality control team, prepare a quality control review checklist from an IS Auditor's perspective.

Audit Tests of General and Automated Controls

11. A Telecom organization produces information on a real-time and online basis which requires real-time auditing on the quality of the data and auditor's assurance testing. Identify the audit tool that tags the online transactions and collects audit evidence in a dummy entity.

12. As an internal auditor of an enterprise, which has acquired and implemented an ERP system in its headquarters and five regional branch offices, how will you perform the testing of general and automated controls on the following issues:

(a) The flow of data and information between the headquarters and the five branch offices,

(b) The concurrent usage of 1000 employees on an average across the offices at anytime, and

(c) The data processing and report generation is in tune with the management objectives.

Risk Assessment Methodologies and Applications

13. An enterprise is in the process of leveraging Information and Communication Technology (ICT) for its business value chain process. As a member of ICT implementation team, prepare the risk assessment lists for the following issues:

    (a) Insurance Coverage, and

    (b) Enterprise-wide Application Software Security.

14. Briefly explain the risk analysis and mitigation measures that a system audit and control professional should consider.

Business Continuity Planning and Disaster Recovery Planning

15. (a) What is Business Continuity Planning? Briefly explain the areas covered by a BCP.

    (b) A backup plan is to be prepared for XYZ company in order to specify the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making a backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recover various systems, and a time frame for the recovery of each system. But the most difficult part in preparing the backup plan is to ensure that all the critical resources are backed up. List the resources that are to be considered in a backup plan.

16. (a) Briefly explain the control measures to ensure Confidentiality, Integrity, and Availability of data.

    (b) Differentiate between Incremental Backup and Mirror Backup.

An Overview of Enterprise Resource Planning (ERP)

17. (a) Explain the characteristics of ERP in brief.

    (b) What is Enterprise Controlling? Briefly explain its modules.

18. Explain the following terms with respect to ERP:

    (a) Business Engineering

    (b) Business Management

    (c) Business Modeling

19. ABC Limited has migrated from traditional systems to new real-time integrated ERP systems. The technical advisor of the company advised the owner that the company should take necessary steps to analyze several types of risks. Explain those risks in brief.

Information Systems Auditing Standards, Guidelines, Best Practices

20. (a) Briefly explain the control and objectives of System Development and Maintenance.

    (b) XYZ company is implementing the Statement of Auditing Standards (SAS) No. 70, Service Organizations, an internationally recognized auditing standard. Briefly explain the benefits to the user organization by its implementation.

21. (a) Explain the control and objectives of Organizational Security in brief.

    (b) Explain the various domains of COBIT, identified for high level control objectives to manage IT resources.

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

22. (a) An Information System Audit Report includes various sections: Title Page, Table of Contents, Summary, Introduction, Findings and Appendices. Explain various elements, included in the 'Introduction' section.

    (b) It is clear from various instances that there are not only many direct and indirect benefits from the use of information systems, but also many direct and indirect risks related to the use of information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. Briefly explain the causes of this gap.

23. (a) Briefly discuss end user computing policies with respect to a sample IS Security Policy.

    (b) Differentiate between the responsibilities of a Facilities Management Security Officer and Divisional System Security Officer with respect to the organizational security structure.

Information Technology (Amended) Act 2008

Note: *The Information Technology (Amended) Act 2008 web link: http://www.icai.org/ resource_file/17796IT_ACT_2008.pdf*

24. (a) Explain the power of Controller to make regulations under Section 89 of the Information Technology (Amended) Act 2008.

    (b) What are the powers of a Police Officer under the Information Technology (Amended) Act 2008 to enter and search etc?

25. (a) Define 'Electronic Signature' and 'Electronic Signature Certificate' in the light of the Information Technology (Amended) Act 2008.

    (b) Briefly explain the Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form as per Section 67 A of the Information Technology (Amended) Act 2008.

SUGGESTED ANSWERS / HINTS

1. **(a)** The information system that is designed to meet the special needs of top-level managers at the strategic level of an organization is the Executive Information System (EIS) – which is sometimes referred to as an Executive Support System (ESS). The special characteristics of this information system with the characteristics of decision support system at the strategic levels of management are the following:

- The Strategic level management is concerned with developing organizational mission, objectives and strategies.
- Decisions made at this level of organization handle problems critical to the survival and success of the organization and are called strategic decisions.
- They have a vital impact on the direction and functioning of the organization as for example decisions on plant location, introduction of new products, making major new fund-raising and investment operations, adoption of new technology, acquisition of outside enterprises and so on.
- A holistic analysis and judgment goes into making strategic decisions at this level.

(b) An executive at this level is the best described as a manager and near the top of the organizational hierarchy who exerts a strong influence on the course taken by the organization. The slots in a firm considered to be executive positions vary from company to company. For example, in many firms, the Chief Information Officer (CIO) is usually an executive who participates in key strategic decisions. In other firms, the CIO is a middle manager (who often has a title other than CIO). And sometimes, the person in charge of an organization is basically a data processing director.

The Executive Roles based on their decision making functionality are strategic planning, tactical planning, and "fire-fighting" activities. An executive needs a certain degree of control to ensure that these activities are carried out properly.

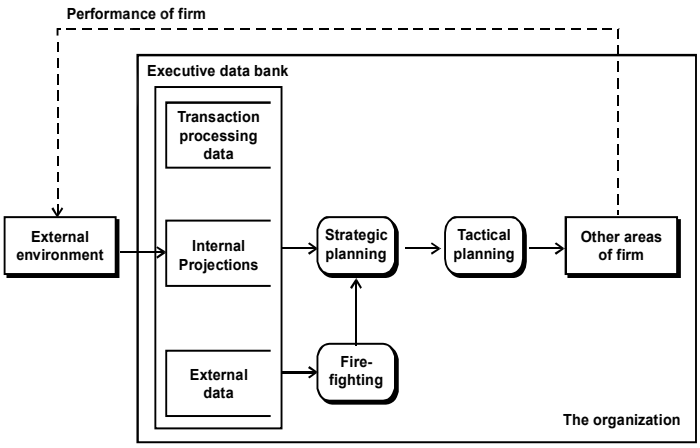

Figure 1

A data flow representation of the executive decision-planning environment is shown in the Figure 1. Corresponding control activities exist for each of the planning functions.

(i) **Strategic Planning:** It involves determining the general, long-range direction of the organization. Typically, the CEO is ultimately responsible for the development of strategic plans.

(ii) **Tactical Planning:** This planning refers to the how, when, where, and what issues involved with carrying out the strategic plan. For example, the vice-president of finance must address how the firm can best achieve a balance between debt and equity financing. And the marketing vice-president will need to consider which classes of products the company should produce to be successful in the marketplace.

(iii) **Fire Fighting:** Major or critical time bound problems arise that requires the efforts of a top-level executive to resolve. For example, if a company is involved in a big lawsuit that threatens its financial solvency, an executive must get involved. Other possible fire-fighting activities include damage caused to a major facility, the announcement of an important product by a competitor, a strike, and a sharp reversal of the economy.

(iv) **Control:** To exert some general control (periodic review) over the organization to achieve a business objective. For example, if the strategic plan calls for a 20 percent increase in profitability, feedback is needed to ensure that certain actions taken within the organization are accomplishing that objective.

2. A **system** functions with a collection of elements organized as a group of interdependent functioning units or components, linked together according to a plan, to achieve a specific objective. These elements surround the system and often interact with it. The feature that defines and delineates a system forms its **boundary**. The system is inside the boundary; the environment is outside the boundary.

A system and its environment can be described with **subsystems** that are a part of a larger system. Each system is composed of subsystems, which in turn are made up of other subsystems, each sub-system being delineated by its boundaries. The interconnections and interactions between the subsystems are termed interfaces. **Interfaces** occur at the boundary and take the form of inputs and outputs.

A complex system is difficult to comprehend when considered as a whole. Therefore the system is decomposed or factored into subsystems. The boundaries and interfaces are defined, so that the sum of the subsystems constitutes the entire system. This process of decomposition is continued within subsystems divided into smaller subsystems until the smallest subsystems are of manageable size.

Doing business is also a system with its components being marketing, manufacturing, sales, research, shipping, accounting and personnel. All these components work together with a common focus to create a profit that benefits the organization.

All systems have some common characteristics that justify the need for decomposition. These are given as follows:

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

An example of the decomposition is the factoring of an information processing system into subsystems. One approach to decomposition might proceed as follows:

(i) Information system divided into subsystem such as:

   a. Sales and order entry
   b. Inventory
   c. Production
   d. Personnel and payroll
   e. Purchasing
   f. Accounting and control
   g. Planning
   h. Environmental intelligence

(ii) Each subsystem is divided further into subsystems. For example, the personnel and payroll subsystem might be divided into the following smaller subsystems:

   a. Creation and update of personnel pay-roll records
   b. Personnel reports
   c. Payroll data entry and validation
   d. Hourly payroll processing
   e. Salaried payroll processing
   f. Payroll reports for management
   g. Payroll reports for government

(iii) If the task is to design and program a new system, the subsystems (major applications) defined in might be further subdivided into smaller subsystems or modules. For example, the hourly payroll processing subsystem as shown in Figure

2, might be factored into modules for the calculation of deductions and net pay, payroll register and audit controls preparation, cheque printing, and register and controls output.

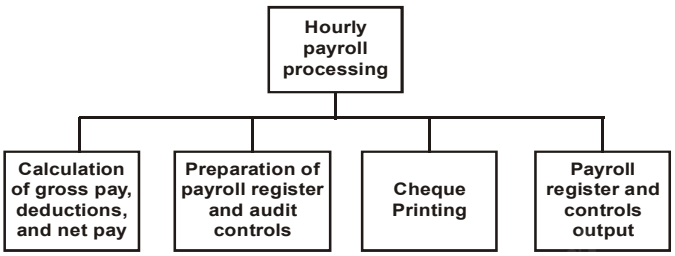

Figure 2

3. (a) Evaluation and validation of the software package to be acquired needs to meet the following features to ascertain before purchasing:

- What is the package designed to do?
- How is the package organized and operable to the present value chain?
- Can the package operate on our hardware configuration?
- Can the program provide the needed reports?
- Does the program have adequate capacity in terms of the number of transactions it can process, the number and length of fields per record it can process, the total file size permitted and so on?
- How many processing runs on the computer are required to complete each data processing job?
- How long does the program take to process?
- Will the package require modifications and how often?
- What are the overall costs on modifications and maintenance?
- Is comprehensive documentation available?
- What are the package constraints?
- Where the package is currently utilized?
- What input/output techniques are utilized?
- What are the required input/output formats?
- What controls are included?
- What kind of user training is provided?

(b) To evaluate and validate the Support Service to be acquired from a vendor, major features to be ascertained are:

- *Performance*: What has been the vendor's past performance in terms of his past promises?

- *System development*: Are system analysis and programming consultants available? What are their qualities and cost?
- *Maintenance*: Is equipment maintenance provided? What is the quality and cost?
- *Conversion*: What systems development, programming and hardware installation service will they provide during the conversion period?
- *Training*: Is the necessary training of personnel provided? What is its quality and cost?
- *Back-up*: Are several similar computer facilities available for emergency back-up purposes?
- *Proximity*: Does the vendor have a local office? Are sales, systems development, programming, and hardware maintenance services provided from the office?
- *Hardware*: Do they have a wide selection of compatible hardware?
- *Software*: Do they have a wide variety of useful systems software application programs?

(c) A Software License Agreement (SLA) is a license that grants permission to do things with computer software. The license is to authorize activities which are prohibited by default by copyright law, patent law, trademark law and any other intellectual property right. The coverage of the license includes:

- The SLA is to encourage disclosure of the intellectual property.
- A method to allow the licensed user to use the product but still be restricted so as to prevent certain decompiling rights the user might otherwise have as a result of the default intellectual property rights.
- It identifies the specific usage rights that are granted to the licensee, while also stating the license limitations.
- A software license is to specify permission to allow a certain number of concurrent users of the software.
- Administrator and user license copies are to be clearly documented.
- A software vendor may offer software license proprietary software sold from a single vendor or a joint agreement with one or more vendors.
- The SLA is to cover the distribution terms under the EULA (End-User License Agreement) is a legal contract between the manufacturer and/or the author and the end user of an application.
- EULA terms are to be followed in a SLA including free software and open source software.
- The SLA should also state the default penalties for violations of intellectual property laws in and if so allowed by the geographic region of the licensor, as well as any terms contractually agreed-upon damages listed in the software license.

4. **(a)** The system development approach that helps organizations to develop smaller systems such as decision support systems, management information systems and expert systems is '**Prototyping'**. The features of this approach are:

- To develop a small or pilot version, called a prototype of part or all of a system.
- A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full-scale and fully operational system.
- As users work with the prototype, they make suggestions about the ways to improve it. These suggestions are then incorporated into another prototype, which is also used and evaluated and so on.
- A prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.
- It helps users to identify additional requirements and needs that they might have overlooked or forgotten to mention and gives a clear visual picture of what the final version will look like.
- Prototyping can be viewed as a series of four steps:

In the given scenario, the steps to be followed for the prototyping are as follows:

(i) *Step 1: Identify Information System Requirements*: The design team needs only fundamental system requirements to build the initial prototype, the team can develop the detailed requirements of the system later after users have had time to interact with the prototype and provide feedback.

(ii) *Step 2: Develop the Initial Prototype*: The designers create an initial base model for example, using fourth-general programming languages or CASE tools. Here the goals are "rapid development" and "low cost." The designers emphasis on system characteristics as "simplicity," "flexibility," and "ease of use."

(iii) *Step 3: Test and Revise*: The initial prototype is demonstrated to users and given to them to experiment. The users are informed that the prototype is incomplete and requires subsequent modifications based on their feedback.

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

(b) The major reasons for choosing the prototyping approach for system development are:

(i) Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.

(ii) A very short time period (e.g., a week) is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.

(iii) Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process.

(iv) The iterative process of modification and reevaluation continues until the users are satisfied, through four to six interactions.

(v) It enables users to interact with tentative versions of data entry display screens, menus, input prompts, and source documents.

(vi) It enables users to be able to respond to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.

(vii) The information system implemented can ensure more reliability with less costly to develop.

(viii) Decision supports semi-structured or unstructured management decision environment, are ideal for the experimentation and trial-and-error development associated with prototyping

(c) With the increasing availability of low-cost technology, end user involvement in development is critical for the successful implementation of information systems in organizations. A clear documentation of end-user requirements during the systems development activities is mandatory. For example, whenever a manager or a department acquires its own, relatively inexpensive micro computers or office information systems, end-user development often takes place.

The risk involved in end-user computing are:

- A decline in standards and controls. When an analyst is in-charge of developments, walk-through will be done and standards and policies will be enforced; these things are unlikely to be carried out to the same degree with end-user computing.
- Inaccuracy of specification requirements. The end-user will not have the experience of an analyst in completing an accurate specification of system requirements.
- Due to the lack of adequate specifications, there would be a reduction in the quality assurance and stability of the system.
- An increase in unrelated and incompatible systems. Departments would choose their own software and hardware and incompatibility of systems would result; this would mean that management would have difficulty in obtaining full corporate data.
- Difficulties in accessing could arise for users trying to access a central system, such as the corporate database, with a proliferation of different systems and applications.

5. The categorization of the controls along with reasons from an Auditor's perspective is as follows:

(a) The user id of an employee who initiates a trans-action is recorded in the database.	Preventive Control	The control prevents malicious act. The user-id is recorded in the database along with the details of the transaction initiated by the user, this help in tracing errors due to data input and prevents critical errors in a financial system.
(b) Hash totals are calculated both at the sender and receiver end of the data transmission network.	Detective Control	This control is designed to avoid omissions or malicious acts that occur and reports the occurrence. A periodic report of error occurrences gives a clear understanding of lawful activities and anything which deviates from these is reported as unlawful and malicious.
(c) Data backup procedures are scheduled for every hour on the customer sales records of the enterprise database.	Corrective Control	This control reduces the impact or corrects an error once it has been detected. This control is a part of a business continuity plan and is considered to be a significant corrective control.
(d) After three attempts of login with wrong password the account is locked for 4 (four) hours.	Preventive Control	This control is implemented to prevent unauthorized access. This preventive control addresses the probable threats in an authentication mechanism.
(e) The employees authorized to enter the server room are given embedded chip-based ID-card.	Compensatory Control	This control is designed to reduce the probability of threats and possible exploitation of the vulnerabilities of accessing the asset and leading to losses. Here the cost of the plastic ID-card is negligible to the cost of the assets. The compensatory measure is not as efficient as the appropriate control but can indubitably reduce the probability of threats to the assets.

6. (a) **Exposure:** Records or files assigned to a particular user being modified by another user.

Access Control Type: Logical access control.

Control Techniques:

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. They restrict users to authorized transactions and functions.

An access control mechanism associates with identified and authorized users to the resources they are allowable to access and action privileges. The mechanism processes the users request for resources in the following sequence:

- First, 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.

The mechanism accesses previously stored information about users, the resources they can access, and the action privileges they have with respect to these resources; it then permits or denies the request.

Users identify themselves to access control mechanism by providing authentication information such as:

Remembered information	Name, Account number, passwords
Objects Possessed by the user	Badge, plastic card, key
Personal characteristics	Finger print, voice print, signature
Dialog	Through/around computer

The authorization module then functions in terms of a matrix where rows represent the users and columns represent the resources and the element represents the user's privilege on the resources:

This mechanism operates via a column in the Authorization matrix:

Resource / User	File A	Editor	File B	Program
User P	Read	Enter		
User Q	Statistical Read only	Enter		Enter

User R		Enter	Append only	
User S		Enter		Read Resource Code only

Each user process has a pointer to the access control list (matrix) for a resource. Thus the capabilities for a resource can be controlled as they are stored in one place. It is enough to examine the access control list just to know who has access over the resource and similarly to revoke access to a resource, a user's entry in the access control list simply needs to be deleted.

(b) **Exposure:** Anybody can enter the server room.

Access Control Type*:* Physical Access Control.

Control Techniques: Physical access controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. These controls should be designed in such a way that it allows access only to authorized persons. The authorization given by the management may be explicit, as in a door lock for which management has authorized a person to have a key; or implicit, like a job description which confirms the need to access confidential reports and documents or a server room.

Some of the more common access control techniques are:

(i) Locks on Doors:

- *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.
- *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 be 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) Physical identification medium

- *Personal Identification numbers (PIN)* **–** A secret number will be assigned to the individual, which serves to verify the authenticity of the individual by

inserting a card in some device and then enter their PIN via a PIN keypad for authentication.

- *Plastic Cards*- These cards are used for identification purposes. Controls over card seek to ensure that customers safeguard their card so it does not fall into unauthorized hands.

(iii) Logging on utilities

- *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.
- *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.

(c) **Exposure**: To change the contents of the web pages published on a company's server.

Access Control Type: Network Access Control.

Control Techniques: Monitoring network to detect week points and multiple communication paths between networks components are done by using preventive maintenance controls. These controls include data encryption, routing verification and message acknowledgement procedures. The implementation of these controls is performed by firewalls and intrusion detection systems (IDSs).

(i) 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).

Here an Application-level firewall will perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. It examines each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers.

(ii) Intrusion Detection Systems: This is placed between the firewall and the system being secured, and provides an extra layer of protection to that system. It monitors access from the internet to the sensitive data ports of the secured system and can determine whether the firewall has perhaps been

compromised, or whether an unknown mechanism has been used to bypass the security mechanisms of the firewall to access the network being protected.

The types of Intrusion Detection systems are:

- *Network based 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.
- *Host based systems.* These types of systems actually run on the system being monitored. These examine the system to determine whether the activity on the system is acceptable.
- *Operating system based:* A more recent type of intrusion detection system are those that reside in the operating system kernel and monitor activity at the lowest level of the system. These systems have recently started becoming available for a few platforms, and are relatively platform specific.

(d) **Exposure:** Failure of hard disks in the database storage system due to spikes in the electrical supply and heating.

Access Control Type: Environmental Access Control.

Control Techniques: The environmental security measures are taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Assessing the environmental protection involves evaluating if the controls have been implemented and are commensurate with the risks of physical damage or access. The control techniques required to mitigate the identified exposure are:

(i) *Electrical Surge Protectors:* The risk of damage due to power spikes are reduced by using electrical surge protectors.

- The incoming current is measured and monitored by the voltage regulator, ensures consistent current.
- These are typically built into the Uninterruptible Power Supply (UPS) system.

(ii) *Uninterruptible Power Supply (UPS) / Generator:* A UPS system consists of a battery or gasoline powered generator that interfaces between the electrical power entering the facility and the electrical power entering the computer.

- It cleanses the power to ensure wattage into the computer is consistent.
- In case of a power failure, the UPS provides the back up by providing electrical power from the generator to the computer for a certain span of time (a few minutes up to few hours) to permit an orderly computer shutdown.

(iii) *Emergency Power-Off Switch*: The need for immediate power shut down arises during situations like a computer room fire or an emergency evacuation, a two emergency power-off switch one at computer room and other near but outside the computer room and easily accessible, yet secured from unauthorized access is mandatory.

(iv) *Humidity/Temperature Control:* Sensors/Alarms in the information processing facility to monitor on regular intervals and determine if temperature and humidity are adequate.

(e) Exposure: The system development projects/tasks consume excessive resources and unauthorized system changes are recorded.

Access Control Type: Change management controls.

Control Techniques: To properly control information system changes, companies need formal change management control policies and procedure. These controls should include the following:

- Periodically review all systems for needed changes and requirements are to be submitted in a standardized format.
- Log and review requests from authorized users for changes and additions to systems.
- Assess the impact of requested changes on system reliability objectives, policies and standards.
- Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is as audit trail for all urgent matters.
- Communication all changes to management and keep change requestors informed of the status of their requested changes.
- Require IT management to review, monitor, and approve all changes to hardware, software, and personnel responsibilities.
- Assign specific responsibilities to those involved in the change and monitor their work. Make sure that the specific assignments result in an adequate segregation of duties.
- Make sure all changes go through the appropriate steps (development, testing, and implementation).
- Test all changes to hardware, infrastructure, and software extensively in a separate, non production environment before placing it into live production mode.
- Make sure there is a plan for backing out of any changes to mission-critical systems in the event that it does not work or does not operate properly.

- Implement a quality assurance function to ensure that all standards and procedures are followed and to assess if change activities achieve their stated objectives. These findings should be communicated to user departments, information systems management, and top management.
- Update all documentation and procedures when changes are implemented.

7. (a) The environmental exposures are primarily due to elements of nature. Common occurrences are Fire, Power spike and Electrical shock which justify the need for the Fire Suppression Systems or alarms. They are activated when extensive heat is generated due to fire. Like smoke alarms they are designed to produce audible alarms when activated and should be regularly monitored. In addition to precautionary measures, 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:

- **Water based systems:** They are sprinkler systems with a continuous supply of water. These systems are effective but also are unpopular because they damage equipment and property in the case of leakage or breakage of pipes the facilities are exposed to extensive water damage.
- **Dry-Pipe sprinkling systems:** These pipes remain dry and upon activation by the electronic fire alarm water is sent through the pipe. Dry pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment.
- **Halon systems:** They contain pressurized halon gases that remove oxygen from the air. It is preferred to others because of its inertness and it does not damage equipment like water does. There should be an audible alarm and brief delay before discharge to permit personnel time to evacuate the area or to override and disconnect the system. The drawback is, since halon adversely affects the ozone layer, its usage is restricted to some extent and alternative suppression methods are being explored.

(b) The Physical Access control techniques that can be implemented to prevent unauthorized access to critical IT infrastructures like server room, storage network devices, and switch/router installations are as follows:

- **Video Cameras:** Cameras should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video supervision recording must be retained for possible future play back.
- **Security Guards**: Extra security can be provided by appointing guards aided with video cameras and locked doors. Guards supplied by an external agency should be made to sign a bond to protect the organisation from loss.
- **Controlled Visitor Access***:* A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.

- **Bonded Personnel***:* All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond. This may not be a measure to improve physical security but to a certain extent can limit the financial exposure of the organisation.
- **Dead man Doors***:* These systems encompasses a pair of doors that are typically found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with only one person permitted in the holding area.
- **Non–exposure of Sensitive Facilities***:* There should be no explicit indication such as presence of windows of directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.
- **Computer Terminal Locks***:* These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.
- **Controlled Single Entry Point***:* A controlled entry point is monitored by personnel. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.
- **Alarm System***:* Illegal entry can be avoided by linking alarm system to inactive entry point motion detectors and the reverse flows of enter or exit only doors, so as to avoid illegal entry.
- **Perimeter Fencing:** Fencing at boundary of the facility may also enhance the security mechanism.
- **Control of out of hours of employee access***:* Employees who are in office for a longer duration exceeding the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently.
- **Secured Report/Document Distribution Cart**: Secured carts, such as mail carts, must be covered and locked and should always be attended.

8. Public Key Infrastructure (PKI) provides a strong means of authentication in an financial organization. The characteristic of PKI are stated below:

- It includes hardware components, system software, policies, practices, and standards.
- PKI is used for authentication, data integrity, defenses against customer repudiation, and confidentiality.
- 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 ke***y.
- The ***public key*** is made available to those who need to verify the user's identity.

- The *private key* is stored on the user's computer or a separate device such as a smart card.
- The key pair is created with strong encryption algorithms and input variables, the probability of deriving the private key from the public key is extremely remote.
- The private key is stored in encrypted text and protected with a password or PIN to avoid compromise or disclosure.
- 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.

The *Certificate Authority* (CA), which may be the financial institution or its service provider, plays a key role by attesting with a *digital certificate* that a particular public key and the corresponding private key belongs to a specific user or system. The issuing of a digital certificate is adequately controlled by a CA with the following procedures.

- The CA attests to the individual user's identity by signing the digital certificate with its own private key, known as the *root ke*y.
- Each time the user establishes a communication link with the financial institution's systems, a digital signature is transmitted with a digital certificate.
- These electronic credentials enable the institution to determine that the digital certificate is valid and confirms that transactions entered into the institution's computer system were performed by an authenticated user.

Whether the financial institution acts as its own CA or relies on a third party, the institution should ensure its certificate issuance and revocation policies and other controls are followed.

When utilizing PKI policies and controls, financial institutions need to consider the following:

- Defining within the certificate issuance policy the methods of initial verification that are appropriate for different types of certificate applicants and the controls for issuing digital certificates and key pairs;
- Selecting an appropriate certificate validity period to minimize transactional and reputation risk exposure—expiration provides an opportunity to evaluate the continuing adequacy of key lengths and encryption algorithms, which can be changed as needed before issuing a new certificate;
- Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions accompanied by a certificate;
- Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a user's private key or the closing of user accounts;
- Updating the database of revoked certificates frequently, ideally in real-time mode;

- Employing stringent measures to protect the root key including limited physical access to CA facilities, tamper-resistant security modules, dual control over private keys and the process of signing certificates, as well as the storage of original and back-up keys on computers that do not connect with outside networks;
- Requiring regular independent audits to ensure controls are in place, public and private key lengths remain appropriate, cryptographic modules conform to industry standards, and procedures are followed to safeguard the CA system;
- Recording in a secure audit log all significant events performed by the CA system, including the use of the root key, where each entry is time/date stamped and signed;
- Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions and unauthorized activities; and
- Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require the acceptance of the financial institution's certificates by other CAs.

9. A user's interface with the information system involves data input/data entry forms, which arise the need for controls during data submission. The Input validation routines mitigate the risks due to invalid or inaccurate data in computer-processed transaction files. The controls to be implemented here are:

- As transaction files are processed, edit programs check key data fields using these edit checks, sequence, field, sign, validity, limit, range, reasonableness, redundant data, and capacity checks.
- Exceptions are recorded in an error log. These are investigated corrected, and resubmitted on a timely basis.
- A summary report is prepared on the error log to re-edit programs or new validation program checks.
- The program checks during a data entry operation may include:
- Field, limit, range, reasonableness, sign, validity, and redundant data checks; user Ids and passwords; compatibility tests; automatic system date entry; prompting operators during data entry, pre-formatting, completeness test; closed-loop verification; a transaction log maintained by the system; clear error messages, and data retention sufficient to satisfy legal requirements.

User controls: required for validity of computer application systems output requires the user responsibility in data submission and for correction of errors that are the result of inaccurately submitted data.

User controls over data being processed should include:

- User instruction manuals defining responsibilities and actions;
- 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 instruction manual should include:

- A narrative description of the system (IT and Manual).
- A detailed flowchart of all clerical processes.
- A detailed document flowchart.
- A copy of each input document, completed as an example, together with instructions for preparation.
- A list of approvals required on each input document.
- A copy of any batch control forms or other transmittal forms used together with instructions on their preparation and reconciliation to batch edits reports.
- A listing of computerized input and processing edits performed the error messages that result there from, and instructions for correcting, resubmitting and balancing the resubmitted items.
- A copy of each report produced by the system with a description of its purpose, the number of copies, distribution and instructions for balancing output to original input
- A list of retention periods for:
  - input source documents
  - data file (tape or disk)
  - output report.
- A system recovery section including user responsibilities for assisting in the restoration of the system.

Error Correction techniques: to be followed are:

- Identify all data and processing errors that can be identified, either through edits or routine processing.
- Determine the impact data and processing errors have on processing (errors must be corrected before processing continues, errors are segregated from processing so good transactions may continue to be processed while errors are corrected).
- Determine if errors are segregated onto a suspense file. Determine if the error suspense file is cumulative or non-cumulative.
- Review the error reports to determine if they are of reasonable length.
- Determine how errors are corrected.

- Determine if the corrected transactions are authorized.
- Verify that the corrected transactions are reintroduced into mainstream processing either at the original point of input or through a special error correction process.
- Determine if the error correction process removes the items from the error suspense file
- Determine the timeliness of error correction.
- Identify how end-users monitor the remaining errors and conduct timely further investigations.
- Is there an appropriate separation of duties (custody, authorization, recording, and periodic reconciliations) for those authorized to update data?
- Determine if all reconciliation and error correction procedures are documented in the end-user documentation.
- Is an exception report generated for long-outstanding error transactions, with an aging analysis?

10. For an IS Auditor, to carry out detailed reviews of system logical design and quality control the general questions to be answered are stated below:

(a) Does system design follow a defined and acceptable standard?

(b) Are completed designs discussed and agreed with the users? (perhaps with the assistance of prototypes);

(c) Does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organization'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 statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?

(g) Are defects uncovered during quality reviews always corrected?

(h) Does the production of development specifications also include the production of relevant acceptance criteria?

(i) Has a Configuration Manager been appointed? Has the configuration management role been adequately defined?

(j) Are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?

(k) Has sufficient IT (in the form of spreadsheets, databases, and specialist configuration management support tools) been provided to assist with the configuration management task?

(l) Are effective procedures in place for recording, analysing and reporting failures uncovered during testing?

(m) Are effective change management procedures are in place to control changes to configuration items?

(n) Has a System Installation Plan been developed and quality reviewed?

(o) Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery? (to avoid "skills stagnation", the delivery of training will need to be carefully scheduled);

(p) Is the system development environment is regularly backed up with copies of backed up configuration items held securely at a remote location?

(q) Are contingency plans commensurate (in terms of time to implement) with the criticality of the project?

(r) Do regular Project Board meetings take place to review project progress against budget and deadline?

Is the Business Case regularly updated to ensure that the project remains viable?

11. A Telecom organization produces information on a real-time, online basis which requires real-time recordings and real-time auditing to ensure continuous assurance about the quality of the data. Continuous auditing enables auditors to significantly reduce and perhaps eliminate the time between occurrence of the client's events and the auditor's assurance services thereon.

Errors in a computerized system are generated at high speeds and the cost to correct and rerun programs are high. If these errors can be detected and corrected at the point or closest to the point of their occurrence, the impact thereof would be the least. The continuous auditing technique to collect audit evidence by tagging transactions is called the **Integrated Test Facility (ITF).**

The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included along with the normal production data and given as input to the application system. The two methods to audit are:

(i) *Methods of Entering Test Data*:

- The transactions to be tested are to be tagged.
- The application system is programmed to recognize the tagged transactions and invoke two updates namely the application system master file record and the ITF dummy entity.

- The live transactions can also be tagged as ITF transactions, provide ease of use and testing with transactions representative of normal system processing.
- Test transactions are entered along with the production input into the application system.
- The test data is likely to achieve a complete coverage of the execution paths in the application system to be tested than a selected production data.

(ii) *Methods of Removing the Effects of ITF Transactions*:

- The presence of ITF transactions within an application system affects the output results obtained.
- The application system is programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users.
- Another method is removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions.
- Otherwise, to submit trivial entries so that the effects of the ITF transactions on the output are minimal.

12. (a) To test the flow of data and information between the headquarters and the five branch offices were an enterprise-wide application is implemented to process the business cycle, the testing method used is called the **Inter System Testing**.

This test method ensures that the data flow and interconnection between the application systems function correctly.

The objectives of this test are:

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

The method of testing involves:

- Operations of multiple systems are tested.
- Multiple systems are run from one another to check that they are acceptable and processed properly.
- The testing also ensures synchronization when there is a change in the parameters of the application system.
- The parameters, which are erroneous and the risk associated to such parameters decide the extent of testing and type of testing.
- Intersystem parameters are checked and verified after the change or when a new application is placed in the production.

(b) To test if concurrent usage of 1000 employees on an average across the offices at anytime is feasible on the implemented ERP system, the **Volume testing method** is followed.

The test method checks the behaviour of the enterprise-wide system when the maximum number of users are logged concurrently and when the database contains the greatest data volume.

This test method involves:

- Creation of a large volume test environment.
- It tests the level of complexity in terms of the data within the database and the range of transactions and data used by the users.
- The test tries to reliably reflect the production environment.
- Volume tests offer much more than simple service delivery measurement.

The test answers the following questions:

- What service level can be guaranteed? How can it be specified and monitored?
- Are changes in user behaviour likely? What impact will such changes have on resource consumption and service delivery?
- Which transactions/processes is resource hungry in relation to their tasks?
- What are the resource bottlenecks? Can they be addressed?
- How much spare capacity is there?
- The volume testing brings out the weaknesses in the system with respect to its handling of large amount of data during extended time periods

(c) **Control testing,** ensures if the data processed and report generation done by the implemented ERP is in tune with the management objectives. It is a management tool to ensure that processing is performed in accordance to management desires or intent. This testing method is used in parallel with the other system tests.

The testing ensures that:

- the data is accurate and complete.
- the transactions are authorized.
- there is adequate maintenance of audit trail information.
- the data processing facilities are efficient, effective and economical.
- the processing tasks meet the needs of the user.

In performing the control testing:

- the system risks are identified.

- the testers determine or anticipate what can go wrong in the application system with a negative approach.
- the risk matrix is developed to identify the risks, controls; segments within application system in which control resides.

13. **Risk assessment** is a critical step in disaster and business continuity planning. It is the process of identifying 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 within the minimum time in case of a disaster. It is a useful technique to assess the risks involved in the event of unavailability of information, to prioritize applications, identify exposures and develop recovery scenarios.

(a) *Insurance coverage list:* The information system insurance policy should be a multi-peril policy, designed to provide various types of coverage. Depending on the individual organization and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:

- 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.
- Software reconstruction: In addition to the cost of media, programming costs for recreating the software should also be covered.
- Extra expenses: The cost incurred for continuing the operations till the original facility is restored should also be covered.
- Business interruption: This applies mainly to centers performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.
- Valuable paper and records: The actual cost of valuable papers and records stored in the insured premises should be covered.
- Errors and omissions: This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmers and other information system personnel.
- 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.
- Media transportation**:** The potential loss or damage to media while being transported to off-site storage/premises should be covered.

(b) All software applications or the enterprise-wide applications are to be inventoried and the critical points of access are identified. Each of the critical application is reviewed to assess its impact on the organization, in case of a disaster. **Appropriate recovery plans** are developed to address the following issues.

(i) *Identifying critical applications*: Amongst the applications currently being processed the critical applications are identified. They are analyzed to determine specific jobs/functions which are critical for smooth functioning of a value chain.

(ii) *Assessing their impact on the organization*: Business continuity planning not only concentrate on business disruption but also take into account organizational functions which may be affected. The areas to be considered are:

- Legal liabilities,
- Interruptions of customer services,
- Losses on assets, and
- Likelihood of fraud and recovery procedures.

(iii) *Determining recovery time-frame*: Critical recovery time period is the time within 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.

The other risks to be assessed are:

- Are updated and acceptable standards, policies and guidelines about application software security distributed to concerned employees and are they adequate?
- Are computer security requirements made explicit during new system development and maintenance work?
- Do functional users and auditors participate in system development and maintenance?
- Is there any standard system development and maintenance methodology and is it followed?
- Are software packages purchased and used?
- Do end-users develop and maintain systems using fourth generation languages?
- Have the application software aspects been audited?

14. As a system audit and control professional, the considerations in analyzing risks include:

- Investigating the frequency of particular types of disasters (often versus seldom).
- Determining the degree of predictability of the disaster.
- Analyzing speed of onset of the disaster (sudden versus gradual).
- Determining the amount of forewarning associated with the disaster.
- Estimating the duration of the disaster.

- Considering the impact of a disaster based on two scenarios; vital records are destroyed or are not destroyed.
- Identifying the consequences of a disaster, such as personnel availability and injuries, loss of operating capability, loss of assets and facility damage.
- Determining the existing and required redundancy levels throughout the organization to accommodate critical systems and functions shall include hardware, information, communication, personnel and services.
- Estimating potential loss on increased operating costs, loss of business opportunities, loss of financial management capability, loss of assets and loss of stockholder's confidence.
- Estimating potential losses for each business function based on the financial and service impact and the length of time the organization can operate without this business function. The impact of a disaster related to a business function depends on the type of outage that occurs and the time that elapses before normal operations can be resumed.
- Determining the cost of contingency planning

As a system audit and control professional, the **risk mitigation measures** will include:

- Factor or casual analysis can help relate characteristics of an event to the probability and severity of the operational losses.
- A causal understanding helps to take appropriate action to control and manage risks because causality is a basis for both action and prediction.
- Cause models help in the implementation of risk mitigation measures and identify events and their impact on losses.
- Calculate reserves and capital requirements.
- Create culture supportive of risk mitigation.
- Strengthening internal controls, including internal and external audit of systems, processes and controls, including IS audit and assurance).
- Setting up operational risks limits (so business will have to reduce one or more of frequency of loss, severity of loss or size of operations).
- Setting up independent operational risk management departments.
- Establishing a disaster recovery plan and backup systems.
- Insurance.
- Outsourcing operations with strict service level agreements so operational risk is transferred.

15. (a) **Business Continuity Planning:** Planning is an activity to be performed before the disaster occurs or it would be too late to plan an effective response. The resulting

outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience. In fact, these consequences may be more severe because of the lost time that results from inadequate planning. After such an event, it is typical for senior management to become concerned with all aspects of the occurrence, including the measures taken to limit losses. Their concerns range from the initiating event and contributing factors, to the response plans, effective contingency planning and disaster recovery coordination. Rather than delegating disaster avoidance to the facilities or building security organizations, it is preferable for a firm's disaster recovery planner(s) to understand fully the risks to operations and the measures that can minimize the probabilities and consequences, and to formulate their disaster recovery plan accordingly.

When a risk manifests itself through disruptive events, the business continuity plan is a guiding document that allows the management team to continue operations. It is a plan for running the business under stressful and time compressed situations. The plan lays out steps to be initiated on occurrence of a disaster, combating it and returning to normal operations including the quantification of the resources needed to support the operational commitments.

Business continuity covers the following areas:

- *Business resumption planning:* The operation's piece of business continuity planning.
- *Disaster recovery planning:* The technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
- *Crisis management:* The overall co-ordination of an organization's response to a crisis in an effective and timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

(b) The resources to be considered in the **backup plan** are:

- **Personnel:** Training and rotation of duties among information system staff to enable them to replace others when required. Arrangements with another company for provision of staff on need.
- **Hardware:** Arrangements with another company for provision of hardware.
- **Facilities:** Arrangements with another company for provision of facilities.
- **Documentation:** Inventory of documentation stored securely on-site and off-site.
- **Supplies:** Inventory of critical supplies stored securely on-site and off-site with a list of vendors who provide all supplies.
- **Data / information:** Inventory of files stored securely on site and off site.

- **Applications software:** Inventory of application software stored on site and off site.
- **System software:** Inventory of system software stored securely on site and off site.

16. (a) The control measures to ensure Confidentiality, Integrity, and Availability of data are as follows:

(i) Confidentiality: Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure storage of important media and data files, installation of audit trails , audit of confidentiality of data.

(ii) Integrity: Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails , audit of adequacy of data integrity.

(iii) Availability: Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programs and training of employees, installation of audit trails , audit of adequacy of availability safeguards.

(b) Incremental Backup: In an incremental backup generation, only the files that have changed since the last full backup / differential backup / 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. Normally, incremental backups are very difficult to restore. We will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

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

17. (a) The key characteristics of a software application to qualify as a true ERP solution are as follows:

- **Flexibility:** An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).
- **Modular & Open**: ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.
- **Comprehensive**: It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.
- **Beyond The Company**: It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.
- **Best Business Practices:** It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organization.

(b) **Enterprise Controlling:** Enterprise can be managed by using an Integrated Enterprise Management. This consists of getting accounting data prepared by subsidiaries for corporate reporting which will be automatically prepared simultaneously within the local books of each subsidiary. This data is transferred to a module called Enterprise Controlling (EC). It allows controlling the whole enterprise from a corporate and a business unit perspective within one common infrastructure. It helps to speed up provision of business control information by fully automated corporate reporting from operative accounting via financial consolidation to management reporting.

It is easy to transfer the data to the EC module to automatically set up consolidated financial statements including elimination of inter-company transactions, currency translation etc.

Enterprise Controlling consists of three modules: EC-CS, EC-PCA, and EC-EIS.

- **EC-CS:** This component is used for financial statutory and management consolidation which also allows fully automated consolidation of investments- even for many companies and complex investment structures.
- **EC-PCA:** Allows to work with internal transfer prices and at the same time to have the right values from company, profit centre, and enterprise perspectives 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 and management reports in parallel. This provides the management with a consistent view of external and internal financial management reports.
- **EC-EIS (Executive Information System):** Executive Information System allows to take financial data from EC-PCA ,EC-CS or any other application and combine with any external data such as market data, industry benchmarks and /or data from non-SAP applications to build a company specific comprehensive enterprise information system .

18. (a) Business Engineering: Business Engineering has come out of merging of two concepts namely Information Technology and Business Process Reengineering. Business Engineering is the rethinking of Business Processes to improve speed, quality and output of materials or services. The emphasis of business engineering is on the concept of Process Oriented Business Solutions enhanced by Client-Server computing in Information Technology. The main focus in business engineering is the efficient redesigning of company's value added chains. Value added chains are a series of connected steps running through a business which when efficiently completed add value to enterprise and customers. Information technology helps to develop business models, which assist in redesigning of business processes. Business Engineering is the method of development of business processes according to changing requirements.

(b) Business Management: ERP merges very well with common business management issues like Business Process Reengineering, total quality management, mass customization, service orientation, and virtual corporation etc. The basic objective of implementing an ERP program is to put in place the applications and infrastructure architecture that effectively and completely supports the enterprise's business plan and business processes. When an enterprise does not have optimized business processes, the ERP implementation needs process reengineering to capture knowledge of the experts into the system and to gain considerable benefits in productivity. The first step in implementation of ERP is the development of a Business process model showing business process as one large

system and the interconnection and sequence of business subsystems or processes that drive it.

(c) **Business Modeling:** 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. We can model Business as a system making the processes, managing their facilities and material as their resources. Information is treated as a vital resource managing other resources.

19. Organizations face several new business risks when they migrate to real-time, integrated ERP systems. Those risks include:

- **Single point of failure:** Since all the organization's data and transaction processing is within one application system and transaction processing is within one application system.
- **Structural changes:** Significant personnel and organizational structures changes associates with reengineering or redesigning business processes.
- **Job role changes:** Transition of traditional user's roles to empowered-based roles with much greater access to enterprise information in real time and the point of control shifting from the back-end financial processes to the front-end point of creation.
- **Online, real-time:** An online, real-time system environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring of re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).
- **Change management:** It is challenging to embrace a tightly integrated environment when different business processes have existed among business units for so long. The level of user acceptance of the system has a significant influence on its success. Users must understand that their actions or inaction have a direct impact upon other users and, therefore, must learn to be more diligent and efficient in the performance of their day-to-day duties. Considerable training is therefore required for what is typically a large number of users.
- **Distributed computing experience:** Inexperience with implementing and managing distributed computing technology may pose significant challenges.

- **Broad system access:** Increased remote access by users and outsiders and high integration among application functions allow increased access to application and data.
- **Dependency on external assistance:** Organization accustomed to in-house legacy systems may find they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to greater risk.
- **Program interfaces and data conversions:** Extensive interfaces and data conversions from legacy systems and other commercial software are often necessary. The exposures of data integrity, security and capacity requirements for ERP are therefore often much higher.
- **Audit expertise:** Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know only a relatively small fraction of the entire ERP's functionality in a particular core module, e.g. FI auditors, who are required to audit the entire organization's business processes, have to maintain a good grasp of all the core modules to function effectively.

20. (a) The control and objectives of System Development and Maintenance 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, and
- *Security in development and support process:* To maintain the security of application system software and information.

(b) User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls. In addition, the user organization also receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

21. (a) The control and objectives of Organizational Security are as follows:

- *Information System Infrastructure*: To manage information security within the organization,
- *Security of third party access*: To maintain the security of organizational information processing facilities and information assets accessed by third parties, and
- *Outsourcing:* To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

(b) Domain of COBIT: There are four broad domains of COBIT which are given as follows:

- *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. Furthermore, the realization of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place. The following table lists the high level control objectives for the Planning and Organization domain.

Plan and Organize

PO1	Define a Strategic IT Plan and direction
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects
PO11	Manager Quality

- *Acquisition and Implementation:* To realize 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.

Acquire and Implement

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

- *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.

Deliver and Support

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

- *Monitoring:* All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's 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.

Monitor and Evaluate

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

22. (a) The elements included in the 'Introduction' section of Information System Audit Report are as follows:

- **Context:** This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.
- **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 and program, the locations visited and 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 to allow the client and auditee to make informed decisions as a result of the report.

(b) The causes of the gap identified between the need to protect the systems and the degree of protection applied, are as follows:

- Widespread use of technology,
- Interconnectivity of systems,
- Elimination of distance, time, and space as constraints,

- Unevenness of technological changes,
- Devolution of management and control,
- Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations, and
- External factors such as legislative, legal, and regulatory requirements or technological developments.

23. (a) The **end user computing policies** with respect to a sample IS Security Policy are given as under:

(i) 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.

(ii) 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.

(iii) Games May Not Be Stored or Used on Computer Systems: Games may not be stored or used on any computer systems.

(iv) 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.

(v) Periodic Review of Software Licensing Agreements: The agreements for all computer programs licensed from third parties must be periodically reviewed for compliance.

(vi) 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.

(b) Facilities Management Security Officer (FMSO): The Facilities Management Security Officer (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.

Divisional System Security Officer (DSSO): A System Security Officer (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 SSOs in their division at the ISMG and for communicating requirements and issues to/from this group.

24. (a) [Section 89] Power of Controller to make Regulations:

(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, 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

(a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (n) [Substituted for (m) vide amendment dated 19/09/2002] of section 18;

(b) the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority under sub-section (1) of section 19;

(c) the terms and conditions subject to which a license may be granted under clause (c) of sub-section (3) of section 21;

(d) other standards to be observed by a Certifying. Authority under clause (d) of section 30;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 34;

(f) the particulars of statement which shall accompany an application under sub-section (3) of section 35

(g) the manner by which a subscriber communicates the compromise of private key to the Certifying Authority under sub-section (2) of section 42.

(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 thirty days which may be comprised in one session or in two or more successive- sessions, and if, before the expiry of the session immediately

following the session or the successive sessions aforesaid, both Houses agree in making any modification in the regulation or both Houses agree that the regulation should not be made, the regulation shall there after have effect only in such modified form or be of no effect, as the ease may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that regulation.

(b) [Section 80] Power of Police Officer and Other Officers to Enter, Search, etc.:

(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 Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and 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 any other place intended for use by, or accessible to the public.

(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.

(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

25. (a) These are the additional definitions added by the Information Technology (Amendment) Act 2008 which are given as follows:

Electronic signature: It means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature

Electronic Signature Certificate: It means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate.

(b) [Section 67 A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008):

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on

first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form:

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes.