DISCLAIMER

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

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

Candidates are also required to answer any five questions

from the remaining six questions.

Question 1

Software development is an integrated process spanning the entire IT organization. ABC Technologies Ltd. is a leading company in the field of software development of various domain. The company is committed to follow System Development Life Cycle (SDLC) with best practices for its different activities. A system development methodology is a formalized, standardized, documented set of activities that analysts, designer and user can come out to develop and implement an information system which contains appropriate controls for all its phases so as to retain records in electronic format with reasonable level of security.

Read the above carefully and answer the following:

(a) As a part of system development team, the system analyst prepare a document called the System Requirement Specification" (SRS). Describe the contents of SRS for a typical software development. (5 Marks)

(b) Describe the provisions for retention of electronic records under Section 7 of Information Technology (Amendment) Act, 2008. (5 Marks)

(c) Explain the role of auditor in information processing system design through SDLC. (5 Marks)

(d) 'Security requirement should be identified and agreed prior to the development of information system. This begins with analysis, specification and provide controls at every stage.' Discuss the 'control and objectives' of system development and maintenance area of information security management. (5 Marks)

Answer

(a) Major contents of a System Requirements Specification (SRS) for a typical software development are given as follows:

- Introduction: It contains goals and objectives of the software in the context of computer-based system and information description.
- Information Description: It contains problem description; information content, flow and structure; hardware, software, human interfaces for external system elements and internal software functions.
- Functional Description: Diagrammatic representation of functions; processing narrative for each function; interplay among functions; design constraints are the major parts of functional description.

- Behavioral Description: It covers responses to external events and internal controls.
- Validation Criteria: It contains classes of tests to be performed to validate functions, performance and constraints.
- Appendix: It may have various items like Data flow / Object Diagrams; Tabular data; detailed description of algorithms, charts, graphs and other such material.
- SRS Review : It contains the following:
  - The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.
  - The review reflects the understanding of the development team about the existing processes. Only after ensuring that the document represents existing processes accurately, the user should sign the document. This is a technical requirement of the contract between users and development team / organization.

(b) Provisions of retention of electronic records under Section 7 of Information Technology (Amendment) Act, 2008 are given as follows:

[Section 7] Retention of Electronic Records:

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

However,

this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records, publication of rules, regulation, etc. in Electronic Gazette.

(c) The role of auditor in information processing systems' design is given as follows:

- To evaluate the appropriateness of the requirements elicitation strategy in the scope of the stakeholders and the quality of the requirements document.
- To ensure that the system design needs to capture all data/information flow within the system.
- To evaluate the structure of the database design and cost of the data model.
- User interface is the source of user interactivity with the system and is a critical activity. Auditor should verify that the design and quality of the interface are following the best design practices.
- To assess the efficiency of the tasks assigned to the appropriate hardware and software resources of the physical design of the system. The performance of a critical system should also be evaluated with the help of simulations.

(d) Major controls and objectives of system development and maintenance area of information security management are given 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 and 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.

Question 2

(a) What facilities are available in Treasury Cash Management of an ERP package? Explain. *(6 Marks)*

(b) Discuss the issues to be addressed in 'Access Control' under information security policy. *(6 Marks)*

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

Answer

(a) In Treasury Cash Management of an ERP package, the company's payment transactions are grouped into cash holdings, cash inflows and cash outflows. The key facilities available in Cash Management module provides:

(i) Information on the sources and uses of funds to secure liquidity to meet payment obligations when they become due.

(ii) Monitors and controls incoming and outgoing payments flows.

(iii) Supplies data required for managing short term market investment and borrowings.

(iv) Enables to know current cash position, short term cash management and medium and long term financial budgeting.

(v) Enables analysis of liquidity.

(vi) Helps in cash management decisions.

(vii) In bank accounting, it helps in electronic banking and control functions for managing and monitoring of bank accounts.

(viii) The liquidity forecast function integrates anticipated payment flows from financial accounting, purchasing and sales to create liquidity outlook from medium to long term.

(ix) Covers foreign currency holdings and foreign currency items.

(b) Major issues to be addressed in 'Access Control' under information security policy are given as follows:

- Access controls must be in place to prevent unauthorized access to information systems and computer applications.
- Access must only be granted in response to a business requirement. Formal processes must be in place to provide individuals with access. The requirement for access must be reviewed regularly.
- System Owners are responsible for approving access to systems and they must maintain records of who has access to a particular system and at what level. The actual access controls in place must be audited against this record on a regular basis.
- Users should be granted access to systems only up to the level required to perform their normal business functions.
- The registration and de-registration of users must be formally managed.
- Access rights must be deleted for individuals who leave or change jobs.
- Each individual user of an information system or computer application will be provided with a unique user identifier (User ID).
- It should not be permitted for an individual to use another person's user ID or to log-in, to allow another individual to gain access to an information system or computer application.

- PCs and terminals should never be left unattended when they are connected to applications or the network. Someone may use the equipment to access confidential information or make unauthorized changes.
- Passwords Policy should be defined and the structure of passwords and the duration of the passwords should be specified. Passwords must be kept confidential and never disclosed to others.
- When using mobile computing facilities, such as laptops, notebooks, etc., special care should be taken to ensure that business information is not compromised, particularly when the equipment is used in public places.

(c) Major strengths of waterfall approach are given as follows:

- This model is ideal for supporting less experienced project teams and project managers or project teams whose composition fluctuates.
- An orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.
- Progress of system development is measurable in this model.
- It conserves resources also.

Question 3

(a) What do you mean by Encryption? Differentiate between private key encryption and public key encryption. (6 Marks)

(b) In a computer-held information system, what types of protection an organization can use to prevent leakage or misuse of information? Explain. (6 Marks)

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

Answer

(a) Encryption: Encryption refers to conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm to convert the original message called Clear Text into a coded equivalent called Cipher Text. At the receiving end, the cipher text is decoded (decrypted) back into clear text. The encryption algorithm uses a key, which is a binary number that is typically from 56 to 128 bits in length. The more bits in the key, the stronger the encryption method. Two general approaches to encryption are private key and public key encryption.

Private Key Encryption: It uses a single key known to both the sender and the receiver of the message. To encode a message, the sender provides the encryption algorithm with the key, which is used to produce a cipher text message. The message enters into the communication channel and is transmitted to the receiver's location, where it is

stored. The receiver decodes the message with a decryption program that uses the same key employed by the sender.

Public Key Encryption: The public key encryption technique uses two different keys: one for encoding messages and the other for decoding them. Each recipient has a private key that is kept secret and a public key that is published. The sender of a message uses the receiver's public key to encrypt the message. The receiver then uses his/her private key to decrypt the message. Users never need to share their private keys to decrypt messages, thus reducing the likelihood that it may fall into the hands of any unauthorized person.

(b) There are two basic types of information protection that an organization can use to prevent leakage or misuse of information, which are given as follows:

Preventative Information Protection: It is based on use of security controls, which itself is a group of three types of controls such as Physical, Logical, and Administrative.

- Physical controls deal with Doors, Locks, Guards, Floppy Disk Access Locks, Cables locking systems to desks/walls, CCTV, Paper Shredders, Fire Suppression Systems,
- Logical controls deal with Passwords, File Permissions, Access Control Lists, Account Privileges, Power Protection Systems, and
- Administrative controls deal with Security Awareness, User Account Revocation, and Policy.

Restorative Information Protection: If an organization cannot recover or recreate critical information systems in an acceptable time period, the organization will suffer and possibly have to go out of business. Hence, the key requirement of any restorative information system protection plan is that the information systems can be recovered. The restorative information protection program must address the following:

- Whether the recovery process has been evaluated and tested recently?
- The time taken for restoration,
- The quantum of productivity loss,
- The strict adherence of plan, and
- The time needed to input the data changes since the last backup.

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

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritization of critical applications and systems.
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.

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

Question 4

(a) Describe the various threats to the computerized environment due to cyber crimes. (6 Marks)

(b) Briefly describe the advantages and disadvantages of continuous auditing techniques. (6 Marks)

(c) Discuss the methodology of developing a Business Continuity Plan. (4 Marks)

Answer

(a) Following are major threats due to cyber-crimes:

- Embezzlement: It is unlawful misappropriation of money or other things of value, by the person to whom it was entrusted (typically an employee), for his/her own use or purpose.
- Fraud: It occurs on account of internal misrepresentation of information or identity to deceive others, the unlawful use of credit/debit card or ATM, or the use of electronic means to transmit deceptive information, to obtain money or other things of value. Fraud may be committed by someone inside or outside the company.
- Theft of proprietary information: It is illegal to obtain of designs, plans, blueprints, codes, computer programs, formulas, recipes, trade secrets, graphics, copyrighted material, data, forms, files, lists, and personal or financial information, usually by electronic copying.
- Denial of service: An action or series of actions that prevents access to a software system by its intended/authorized users or causes the delay of its time-critical operations or prevents any part of the system from functioning is termed as 'DoS'. There can be disruption or degradation of service that is dependent on external infrastructure. Problems may erupt through internet connection or e-mail service

those results in an interruption of the normal flow of information. DoS is usually caused by events such as ping attacks, port scanning probes, and excessive amounts of incoming data.

- Vandalism or sabotage: It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.
- Computer virus: Viruses are hidden fragments of computer codes, which propagate by inserting themselves into or modifying other programs.
- Others: Threat includes several other cases such as intrusion, breaches and compromises of the respondent's computer networks (such as hacking or sniffing) regardless of whether damage or loss were sustained as a result.

(b) Major advantages of continuous audit techniques are as under:

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

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

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

- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

(c) The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The methodology emphasises on the following:

(i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;

(ii) Obtaining commitment from appropriate management to support and participate in the effort;

(iii) Defining recovery requirements from the perspective of business functions;

(iv) Documenting the impact of an extended loss to operations and key business functions;

(v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;

(vi) Selecting business continuity teams that ensure the proper balance required for plan development;

(vii) Developing a business continuity plan that is understandable, easy to use and maintain; and

(viii) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

Question 5

(a) Describe the major pre-requisites of a Management Information System to make it an effective tool. *(6 Marks)*

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

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

Answer

(a) Major pre-requisites of a Management Information System (MIS) to make it an effective tool are given as follows:

- Database: It is a super-file, which consolidates data records formerly stored in many data files. The data in database is organized in such a way that access to the data is improved and redundancy is reduced. The database should be user-oriented, capable of being used as a common data source, available to authorized persons only and should be controlled by a separate authority such as DBA. Such a database is capable of meeting information requirements of its executives, which is necessary for planning, organizing and controlling the operations of the business.
- Qualified System and Management Staff: MIS should be manned by qualified officers. These officers who are experts in the field should understand clearly the views of their fellow officers. The organizational management base should comprise of two categories of officers (i) System and Computer experts and (ii) Management experts, who should clearly understand the concepts and operations of a computer.
- Support of Top Management: An MIS becomes effective only if it receives the full support of top management. To gain the support of top management, the officer should place before them all the supporting facts and state clearly the benefits which will accrue from it to the concern.
- Control and Maintenance of MIS: Control of the MIS means the operation of the system as it was designed to operate. Sometimes users develop their own procedures or shortcut methods to use the system, which reduces its effectiveness. To check such habits of users, the management at each level in the organization should device checks for the information system control.

  Maintenance is closely related to control. There are times when the need for improvements to the system will be discovered. Formal methods for changing and documenting changes must be provided.
- Evaluation of MIS: An effective MIS should be capable of meeting the information requirements of its executives in future as well. The capability can be maintained by evaluating the MIS and taking appropriate timely action.

(b) Various categories of software maintenance are given as follows:

- Scheduled maintenance: Scheduled maintenance is anticipated and can be planned; for example, implementation of a new inventory coding scheme can be planned in advance.
- Rescue maintenance: Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested, should have few occasions of rescue maintenance.
- Corrective maintenance: Corrective maintenance deals with fixing bugs in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors.

- Adaptive maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The need for adaptive maintenance can only be recognized by monitoring the environment.
- Perfective maintenance: Perfective maintenance mainly deals with accommodating to new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- Preventive maintenance: Preventive maintenance concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

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

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

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

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

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

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

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

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

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

Question 6

(a) Explain the various financial control techniques used in information system control. (6 Marks)

(b) An owner of a small local store is currently using manual system for his day to day business activities viz. purchase, sales, billing, payments receipts etc. In the last few years, turnover of the store is increased manifold and now it has become increasingly difficult to handle all these activities manually. You being an IT expert and his auditor, are

requested to suggest which operation support system will be most suitable for him. Also advise him what activities can be performed by the proposed system and what are major limitation of it. *(6 Marks)*

(c) As per legal theory of Torts, which kind of insurance you would suggest to cover risk of loss? Briefly explain. *(4 Marks)*

Answer

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

- *Authorization*: This entails obtaining the authority to perform some act typically access to such assets as accounting or application entries.
- *Budgets*: These estimates the amount of time or money expected to be spent during a particular period of time, project, or event. The budget alone is not an effective control-budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
- *Cancellation of documents*: This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.
- *Documentation:* This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.
- *Dual control:* This entails having two persons simultaneously access an asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
- *Input/ output verification:* This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.
- *Safekeeping:* This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- *Segregation of duties*: This entails assigning similar functions to separate people to provide reasonable assurance against fraud and provide an accuracy check of the other persons work.
- *Sequentially numbered documents:* These are working documents with preprinted sequential numbers, which enables the detection of missing documents.

- *Supervisory review:* This refers to review of specific work by a supervisor but what is not obvious is that this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them.

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

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

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

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

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

(c) As per legal theory of torts, Third Party Insurance – General Liability is suggested to cover the risk of loss.

Third party insurance is designed to protect the insured from claims of wrongs committed upon others. It is based on the legal theory of torts. Torts are civil wrongs, which generally fit into three categories:

- Intentional,
- Negligent and
- Strict liability.

Intentional torts are generally excluded from liability insurance policies because they are foreseeable and avoidable by the insured. Strict liability torts, such as product liability issues, are generally covered under specialized liability insurance. Generally liability policies include comprehensive, umbrella and excess liability policies. Insured parties are exposed to the risk of liability whenever they violate some duty imposed on, or expected of, parties' relative to each other or society in general.

In the cyber environment, this can take many forms. If the insured's computer damages another party's computer, data connectivity, then the insured may be held liable. A company might be held liable if the computer system was used in connection with a denial-of-service attack. The insured may be also held liable for failing to protect adequately the privacy interests of parties who have been entrusted information to the care of the insured.

Question 7

Write short notes on any four of the following:

(a) Continuous and Intermittent Simulation (CIS)

(b) HIPPA

(c) Risk Assessment

(d) Information System (IS) security objective

(e) COBIT 5 Enablers

Answer

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

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

(b) HIPAA: Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. Major points are given as follows:

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and

national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system. One of the major aspects of this Act is Security Rules issued under the same.

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

Risk assessment is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well-tested contingency plan. Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritize applications, identify exposures and develop recovery scenarios.

(d) Information System Security Objective: The objective of information system security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity, and availability".

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

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

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

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

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

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

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

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

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

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

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