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.*
Wherever necessary suitable assumptions may be made and disclosed by way of a note.

Working notes should form part of the answer.

Question 1

ABC Appliances Limited is a popular marketing company, which has many branches located in different places. It does all its business activities such as receiving orders, placing orders, payments, receipts etc. through online. With increased business activities, the company faces several problems with the existing information system. It realizes that the existing system is outdated and needed improvement. Hence, it wishes to enhance the existing system with adequate measures for information security in order to ensure the smooth functioning of new information system and protect the company from loss or embarrassment caused by security failures. To develop such a new system, the company has formed a system development team with professionals like project managers, system analysts and system designers. The team has executed all the phases involved in the SDLC and implemented the new system successfully. Finally, the Post Implementation Review has also been conducted to determine whether the new system adequately meets present business requirements and the company is satisfied with the PIR report.

Read the above carefully and answer the following:

(a) State the advantages of SDLC from the perspective of the IS Audit. (5 Marks)

(b) Being an IS Auditor, what objectives can you set for the audit of systems under development and how can you achieve your objectives? (5 Marks)

(c) Suggest some points that may be considered for establishing better information protection. (5 Marks)

(d) What are the activities to be undertaken during the Post Implementation Review? (5 Marks)

Answer

(a) From the perspective of the IS Audit, the following are the major advantages of SDLC:

- The IS Auditor can have the clear understanding of the various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
- The IS Auditor on the basis of his/her examination, can state in his/her report about the compliances by the IS management of the procedures, if any, set up by the management.
- The IS Auditor, if has a technical knowledge and ability of the area/s of SDLC, can be a guide during various phases of SDLC.

- The IS Auditor can provide an evaluation of the methods and techniques used during various development phases of the SDLC.

(b) The audit of systems under development can have the following main objectives:

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

For the first objective to achieve, an auditor will have to attend project and steering committee meetings and examine project control documentation and conducting interviews. This is to ensure what project control standards are to be complied with, (such as a formal systems development process) and determining the extent to which compliance is being achieved.

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

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

(c) Major points that may be considered for establishing better information protection are given as follows:

- Not all data has the same value: Each data has a different value and accordingly, the information may be handled and protected differently. Organizations must determine the value of the different types of information in their environment before they plan for the appropriate levels of protection.
- Know where the critical data resides: Identification of the location where each data is located enables an organization to establish an integrated security solution. Protection solution must be based on the most valuable information assets The network environment also present additional challenges for protecting information.
- Develop an access control methodology: Information does not have to be removed to cause damage or to have financial impact. Information that is inadvertently damaged, disclosed or copied without the knowledge of the owner may render the data useless. To guard against this, organizations must establish

some type of access control methodology. There are many solutions available to provide this protected access.

- Protect information stored on media: Employees can cause considerable damage by walking out the door with information on USB Drives or CD-ROMS. In addition, companies should control magnetic media to reduce the loss of software (both application and operating system) and finally, when migrating from one platform to another, the status of all hard drives and the associated data should be controlled.
- Review hardcopy output: The hardcopy output of employees' daily work should also be reviewed. In addition, 'what measures are used to safeguard all drafts and working papers' should also be reviewed.

(d) During the Post Implementation Review, the team should, according to their terms of reference, review:

- the main functionality of the operational system against the User Requirements Specification along with the confirmation that all the anticipated benefits, both tangible and intangible, have been delivered;
- system performance and operation;
- the development techniques and methodologies employed;
- estimated time-scales and budgets, and identify reasons for variations, if any;
- changes to requirements, and confirm that they were considered authorized and implemented in accordance with change and configuration management standards; and
- the findings, conclusions and recommendations documented in a report for the authorizing authority to consider.

Question 2

(a) XYZ Ltd. is a large multinational company with offices in many locations. It stores all its data in just one centralized computer centre. It uses Internal Controls in order to asset safeguarding, data integrity, system efficiency and effectiveness. What could be the interrelated components of its Internal Control? Discuss them briefly. *(6 Marks)*

(b) What is meant by EIS? What are its characteristics? *(6 Marks)*

(c) Explain any four features of Electronic Mail. *(4 Marks)*

Answer

(a) Internal controls used within XYZ Ltd. may comprise of the following five interrelated components:

- Control environment,

- Risk assessment,
- Control activities,
- Information and communication, and
- Monitoring.

A brief overview of each component is given as follows:

- *Control environment*: These are the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.
- *Risk assessment:* This relates to the elements that identify and analyze the risks faced by an organization and the ways the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organization.
- *Control activities:* These are the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of recorded amounts occur. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.
- *Information and communication:* These are related to the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.
- *Monitoring:* These are the elements for ensuring that internal controls operate reliably over time.

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

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

- EIS is a Computer based information system that serves the information needs of top executives.
- EIS enables users to extract summary data and model complex problems without the need to learn query languages, statistical formulas or high computing skills.

- EIS provides rapid access to timely information and direct access to management reports.
- EIS is capable of accessing both internal and external data.
- EIS provides extensive online analysis tools like trend analysis, market conditions etc.
- EIS can easily provide a DSS support for decision making.

(c) Major features of an Electronic Mail are given as follows:

- Electronic transmission: The transmission of messages with email is electronic and message delivery is very quick, almost instantaneous. The confirmation of transmission is also quick and the reliability is very high.
- Online development and editing: The email message can be developed and edited online before transmission. The online development and editing eliminates the need for the use of paper/s in communication. It also facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
- Broadcasting and Rerouting: Email permits sending a message to a large number of target recipients. Thus, it is easy to send a circular to all the branches of a bank using Email resulting in a lot of saving of papers. The email could be rerouted to people having direct interest in the message with or without changing or/and appending related information to the message.
- Integration with other Information systems: The E-mail has the advantage of being integrated with the other information systems. Such an integration helps in ensuring that the message is accurate and the information required for the message is accessed quickly.
- Portability: Email renders the physical location of the recipient and sender. The email can be accessed from any Personal computer equipped with the relevant communication hardware, software and link facilities.
- Economical: The advancements in communication technologies and competition among the communication service providers have made Email the most economical mode for sending messages. Since the speed of transmission is increasing, the time and cost on communication media per page is falling further, adding to the popularity of email. The email is proving to be very helpful not only for formal communication but also for informal communication within the business enterprise.

Question 3

(a) Threat is any circumstance or event with the potential to cause harm to an information system. What can be the threats due to cyber crimes? *(6 Marks)*

(b) What is the skill set expected from an IS Auditor? *(6 Marks)*

(c) In Information Technology (Amended) Act 2008, what do Section 25 and Section 26 say about suspension of license to issue electronic signature certificate? (4 Marks)

Answer

(a) Following are the 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 the 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 (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 that result in an interruption of the normal flow of information. DoS is usually caused by the 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) The skill set expected from an IS auditor includes the following:

- Sound knowledge of business operations, practices and compliance requirements,
- Should possess the requisite professional technical qualification/s and certification/s;
- A good understanding of information Risks and Controls;
- Knowledge of IT strategies, policies and procedure controls;
- Ability to understand technical and manual controls relating to business continuity; and

- Good knowledge of Professional Standards and best practices of IT controls and security.

(c) As per *Section 25 of the Information Technology (Amended) Act, 2008,* the Controller may revoke a license on the grounds such as incorrect or false material, particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made there under.

However, no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

Also, no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

Thereafter, as per Section 26 Information Technology (Amended) Act, 2008, Controller shall publish a notice of suspension or revocation of license as the case may be in the database maintained by him.

Further, the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site, which shall be accessible round the clock.

It is also provided that the Controller may, if he considers necessary, publicize the contents of database in such electronic or other media, as he may consider appropriate.

Question 4

(a) Access to information and business processes should be controlled on the business and security requirements. In that case, what can be the detailed control and objectives with respect to Information Security Management Standard? (6 Marks)

(b) During the review of hardware, how will you review the change in the management controls? (6 Marks)

(c) Describe the duties of certifying authority in respect of Digital Signature under Section 30 of Information Technology (Amended) Act 2008. (4 Marks)

Answer

(a) The detailed controls and objectives of Access Control with respect to Information Security Management Standard/System are given as follows:

- *Business requirement for access control :* To control the access to the information;
- *User access management :* To prevent unauthorized access to the information systems;
- *User responsibilities :* To prevent unauthorized user access;
- *Network access control :* Protection of networked services;

- *Operating system access control : To prevent unauthorized computer access;*
- *Application Access Control : To prevent unauthorized access to information held in information systems;*
- *Monitoring System Access and use : To detect unauthorized activities; and*
- *Mobile Computing and teleworking: To ensure information security when using mobile computing & teleworking facilities.*

(b) During the review of hardware, review in the change in management controls is accomplished by the following:

- Determine if changes to hardware configuration are planned and timely information is given to the individual/s responsible for scheduling.
- Determine whether the change schedules allow time for adequate installation and testing of new hardware.
- Verify that the operator documentation is appropriately updated to reflect the changes in the hardware.
- Select samples of hardware changes that have affected the scheduling of IS processing and determine if the plans for changes are being addressed in a timely manner.
- Ensure that there is a cross-reference between the change and its cause, i.e. the problem.
- Ascertain whether the system programmers, application programmers and the IS staff have been informed about all the hardware changes to ensure that changes are coordinated properly.

(c) [Section 30] Duties of Certifying Authorities of Information Technology (Amended) Act, 2008:

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

Every Certifying Authority shall-

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse:

(b) provide a reasonable level of reliability in its services which arc reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (Amended vide ITAA 2008)

(ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)

(cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)

(d) observe such other standards as may be specified by regulations.

Question 5

(a) Any system has to possess few key characteristics to qualify for a true Enterprise Resource Planning Solution. What are they? *(6 Marks)*

(b) What are the characteristics of a good coded program ? *(6 Marks)*

(c) What are the points to be included when the documented audit program is developed? *(4 Marks)*

Answer

(a) To qualify for a true Enterprise Resource Planning (ERP) solution, a system has to possess the following key characteristics:

- Flexibility,
- Modular and Open,
- Comprehensive,
- Beyond the Company, and
- Best Business Practices.

A brief discussion on each characteristic is given 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. It means, 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 the 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) A good coded program should have the following characteristics:

- Reliability: It refers to the consistency, which is provided by a program over a period of time. However, poor setting of parameters and hard coding of some data subsequently could result in the failure of a program after some time.
- Robustness: It refers to the process of taking into account all the possible inputs and outputs of a program in case of least likely situations.
- Accuracy: It refers not only to 'what program is supposed to do', but should also takes care of 'what it should not do'. The second part becomes more challenging for quality control personnel and auditors.
- Efficiency: It refers to the performance, which should not be unduly affected with the increase in input values.
- Usability: It refers to a user-friendly interface and easy-to-understand document required for any program.
- Readability: It refers to the ease of maintenance of program even in the absence of the program developer.

(c) The points to be included when a documented audit program is developed are given as follows:

- Documentation of the information system auditor's procedures for collecting, analyzing, interpreting, and documenting information during the audit;
- Objectives of the audit;
- Scope, nature, and degree of testing required to achieve the audit objectives in each phase of the audit;
- Identification of technical aspects, risks, processes, and transactions, which should be examined; and
- Procedures for audit prepared prior to the commencement of the audit work and modified, as appropriate, during the course of the audit.

Question 6

(a) What is the scope of IS Audit process? Explain the categories of IS Audit. *(6 Marks)*

(b) What are the elements to be included in the methodology for the development of disaster recovery / business resumption plan? *(6 Marks)*

(c) What are the goals of Business Continuity Plan ? *(4 Marks)*

Answer

(a) The scope of IS Audit process should include the examination and evaluation of the adequacy and effectiveness of the system of internal controls and the quality of performance by the information system. In addition, IS Audit process will also examine

and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists so that objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The scope of the audit will also include the internal control system/s for the use and protection of information and the information systems, such as, *Data, Application systems, Technology, Facilities, and People.*

IS Audit has been categorized into the following five major types:

- Systems and Applications: An audit to verify that systems and applications are appropriate, efficient, and adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.
- Information Processing Facilities: An audit to verify that the processing facility is controlled to ensure timely, accurately, and efficiently processing of applications under normal and potentially disruptive conditions.
- Systems Development: An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- Management of IT and Enterprise Architecture: An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.
- Telecommunications, Intranets, and Extranets: An audit to verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

(b) The elements to be included in the methodology for the development of a disaster recovery/business resumption plan are given as follows:

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

- Determining that the plan is realistic in its assumptions.

(c) The goals of a Business Continuity Plan should be to:

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

Question 7

Write short notes on any four of the following:

(a) Business Engineering (4 Marks)

(b) Constitution of Cyber Regulations Advisory Committee under Section 88 of Information Technology (Amended) Act 2008 (4 Marks)

(c) Limitations of MIS (4 Marks)

(d) Basic ground rules for protecting computer held information system (4 Marks)

(e) Domains of COBIT (4 Marks)

Answer

(a) Business Engineering: The term 'Business Engineering' has emerged by merging the two concepts namely, Information Technology and Business Process Reengineering. Business Engineering is the method of development of business processes according to changing requirements.

Business Engineering is the rethinking of Business Processes to improve the speed, quality and output of materials or services. The emphasis of business engineering is on the concept of Process Oriented Business Solutions enhanced by the Client-Server computing through Information Technology. The main point 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 the enterprise and customers. Information technology helps to develop business models, which assists in redesigning the business processes.

(b) [Section 88] Constitution of Advisory Committee of Cyber regulations of Information Technology (Amended) Act, 2008:

(1) The Central Government shall, as soon as may be after the commencement of this Act, constitute a Committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairperson and such number of other official and non-official members representing the interests

principally affected or having special knowledge of the subject-matter as the Central Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advise –

(a) the Central Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act

(4) There shall be paid to the non-official members of such Committee such traveling and other allowances as the Central Government may fix.

(c) Limitations of MIS: Major limitations of MIS are given as follows:

- The quality of the output of MIS is basically governed by the quantity of input and processes.
- MIS is not a substitute for effective management; it means that it cannot replace managerial judgment in the decision making for different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of the time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decisions made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of the organization, which have an important bearing on the decision making process of executives.
- MIS is less useful for making non-programmed decisions. Such type of decisions is not of the routine type and thus requires information, which may not be available from existing MIS to executives.
- The effectiveness of MIS may be reduced in the organizations, where the culture of hoarding information and not sharing with other holds exist.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

(d) Basic Ground rules for protecting Computer held Information System: A few basic ground rules for protecting Information Systems that must be addressed sequentially are given as follows:

- Rule #1: We need to know that 'what the information systems are' and 'where these are located'.

- Rule #2: We need to know the 'value of the information held' and 'how difficult it would be to recreate if it were damaged or lost'.
- Rule #3: We need to know that 'who is authorized to access the information' and 'what they are permitted to do with the information'.
- Rule #4: We need to know that 'how quickly information needs to be made available and should it become unavailable for whatever reason (loss, unauthorized modification, etc.)'

(e) Domains of COBIT: COBIT covers four domains, which are given as follows:

- Plan and Organize: The Plan and Organize domain covers the use of IT and how best it can be used in a company to achieve the company's goals and objectives. It also highlights the organizational and infrastructural form in order to achieve the optimal results and to generate the maximum benefits from the use of IT.
- Acquire and Implement: The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adapt in order to prolong the life of an IT system and its components.
- Deliver and Support: The Deliver and Support domain focuses on the delivery aspects of IT. It covers areas such as the execution of the applications within the IT system and its results as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training.
- Monitor and Evaluate: The Monitor and Evaluate domain deals with a company's strategy in assessing the needs of the company and whether or not the current system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet the business objectives and the company's control processes by internal and external auditors.