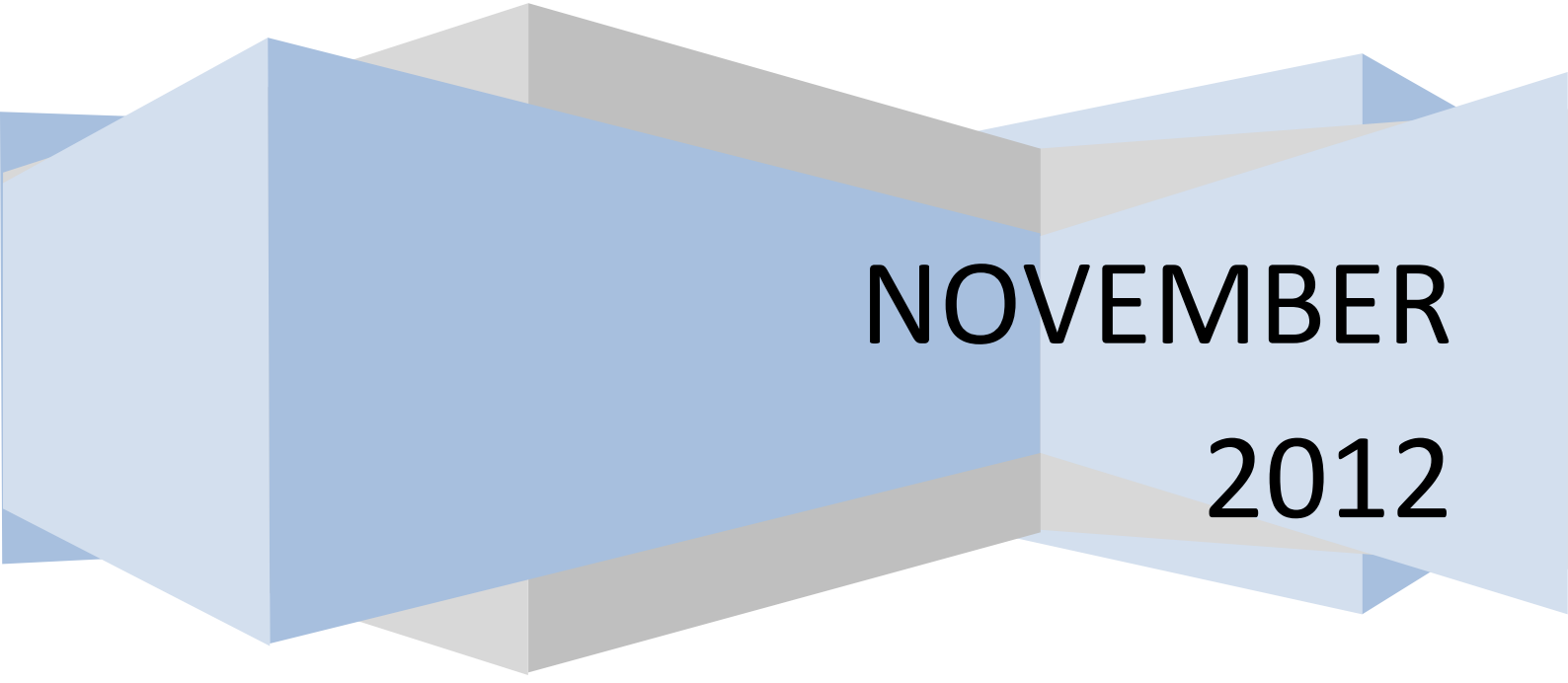
Paper 6

Suggested Answer

ISCA

A HELPING HAND

NO ONE PLANS TO FAIL; BUT FAILS TO PLAN



NOVEMBER 2012

Suggested Answers Nov 2012 ISCA Paper 6

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 It realizes that the existing system is outdated' and needed improvement.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? (Marks5)

(b) Being an IS Auditor, what objectives can you set for the audit of systems under development and how can you achieve your objectives? (Marks5)

(c) Suggest some points that may be considered for establishing better information protection. (Marks5)

(d) What are the activities to be undertaken during the Post Implementation Review? (Marks5)

ANSWERS

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

i. The IS auditor can have clear understanding of the various phases if the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
ii. The IS Auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.
iii. The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.
iv. The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

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

- to provide an opinion on the efficiency, effectiveness, and economy of project management;
- to assess the extent to which the system being developed provides for 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 second objective, the auditor is 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 the 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.

An Auditor may adopt a rating system such as on scale of 1 to 10 in order to give rating to the various phases of SDLC. E.g. in rating a Feasibility Study, auditor can review Feasibility Study Report and different work products of this study phase. An interview with personnel who have conducted this feasibility study can be conducted. Depending on the content and quality of the Feasibility Study report and interviews, an auditor can arrive at a rating from 1 to 10 (10 being best). After deriving such a rating for all the phases, the auditor can form his/her overall opinion about the SDLC phases.

In order to audit technical work products (such as database design or physical design), auditor may opt to include a technical expert to seek his/her opinion on the technical aspects of SDLC. However, auditor will have to give control objectives, directives and in general validate the opinion expressed by technical experts. Some of the control considerations for an auditor are:

- Documented policy and procedures;
- Established Project team with all infrastructure and facilities ;
- Developers/ IT managers are trained on the procedures ;
- Appropriate approvals are being taken at identified mile-stones;
- Development is carried over as per standards, functional specifications;
- Separate test environment for development/ test/ production / test plans;
- Design norms and naming conventions are as per standards and are adhered to;
- Business owners testing and approval before system going live;
- Version control on programs;
- Source Code is properly secured;
- Adequate audit trails are provided in system; and
- Appropriateness of methodologies selected.

Further, Post-Implementation Review is performed to determine whether the system adequately meets earlier identified business requirements and needs (in feasibility studies or Requirements Specifications). Auditors should be able to determine if the expected benefits of the new system were realized and whether users are satisfied with the new system. In post implementation review, auditors need to review which of the SDLC phases have not met desired objectives and whether any corrective actions were taken. If there are differences between expectations and actual results, auditors need to determine the reasons for the same. E.g. it could be due to incomplete user requirements. Such reasons can help auditors to evaluate the current situation and offer guidelines for future projects.

Master Checklist

The process objectives are:

· To ensure an appropriate acquisition and / or development of information systems including software, and

To maintain the information systems in an appropriate manner.

(c) Types of Information Protection: The two basic types of information protection that an organization can use are given as follows:

1. **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.

2. **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 claim of back program to backup data automatically cannot be reliable. It has so many problems. 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.

(d) Objective: To assess and review the complete working solution

Activities: Some of the Systems maintenance activities are as follows:

· Adding new data elements;

· Modifying reports;

· Adding new reports; and

· Changing calculations.

Document / Deliverable: A document stating scope of further improvements, if any like-

- Could further training or coaching improve the degree of benefit being generated?
- Are there further functional improvements or changes that would deliver greater benefit?
- Are specific improvements required in procedures, documentation, support, etc?
- What learning points are there for future projects?

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. (Marks6)

(b) What is meant by EIS? What are its characteristics? (Marks6)

(c) Explain any four features of Electronic Mail? (Marks4)

(a) The internal controls within an enterprise in a computerised environment the major areas of impact with the goal of asset safeguarding, data integrity, system efficiency and effectiveness are discussed below.
(i) *Personnel* : Whether or not staffs are trustworthy, if they know what they are doing and, if they have the appropriate skills and training to carry out their jobs to a competent standard.

(ii) *Segregation of duties* : a key control in an information system. Segregation basically means that the stages in the processing of a transaction are split between different people, such that one person cannot process a transaction through from start to finish. The various stages in the transaction cycle are spread between two or more individuals. However, in a computerised system, the auditor should also be concerned with the segregation of duties within the IT department. Within an IT environment, the staff in the computer department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output. IT staff may also be in a position to alter transaction data or even the financial applications which process the transactions. This gives them the knowledge and means to alter data, all they would then require is a motive.

(iii) *Authorisation procedures* : to ensure that transactions are approved. In some on-line transaction systems written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals)

(iv) *Record keeping* : the controls over the protection and storage of documents, transaction details, and audit trails etc.

(v) *Access to assets and records* : In the past manual systems could be protected from unauthorised access through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs are vulnerable to unauthorised amendment at the computer or from remote locations. The use of wide area networks, including the Internet, has increased the risk of unauthorised access. The nature and types of control available have changed to address these new risks.

(vi) *Management supervision and review* : Management's supervision and review helps to deter and detect both errors and fraud.

(vii) *Concentration of programs and data* : Transaction and master file data (e.g. pay rates, approved suppliers lists etc.) may be stored in a computer readable form on one computer installation or on a number of distributed installations. Computer programs such as file editors are likely to be stored in the same location as the data. Therefore, in the absence of appropriate controls over these programs and utilities, there is an increased risk of unauthorised access to, and alteration of financial data. The computer department may store all financial records centrally. For example, a large multinational company with offices in many locations may store all its computer data in just one centralised computer centre. In the past, the financial information would have been spread throughout a client's organisation in many filing cabinets. If a poorly controlled computer system was compared to a poorly controlled manual system, it would be akin to placing an organisation's financial records on a table in the street and placing a pen and a bottle of correction fluid nearby. Without adequate controls anyone could look at the records and make amendments, some of which could remain undetected.

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

Control environment : 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 : Elements that identify and analyze the risks faced by an organisation and the ways the risk can be managed. Both external and internal auditors are concerned with errors or irregularities cause material losses to an organisation.

Control activities : 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 : Elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.

Monitoring : Elements that ensure internal controls operate reliably over time.

(b) An Executive Information System (EIS) is a tool that provides direct on-line access to relevant information in a useful and navigable format. The relevant information is timely, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager. An EIS is easy to navigate so that managers can identify broad strategic issues, and then explore the information to find the root causes of those issues.

EIS serves the following purpose:

(i) The primary purpose of an Executive Information System is to support managerial learning about an organization, its work processes, and its interaction with the external environment.

(ii) A secondary purpose is to allow timely access to information so that based on the answers to questions, strategic decisions could be taken by a manger in time.

(iii) It directs the attention of the management to specific areas of the organization or specific business problems. It makes managers and subordinates to work together to determine the root causes of issues highlighted by EIS

(c) Four features of Electronic Mail

i. **Electronic transmission :** The transmission of messages with email is electronic andmessage delivery is very quick, almost instantaneous. The confirmation of transmissionis also quick and the reliability is very high.
ii. **Online development and editing :** The email message can be developed and edited online before transmission. The online development and editing eliminates the need for use of paper in communication. It also facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
iii. **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 branches of a bank using Email resulting in a lot of saving of paper. The email could e rerouted to people having direct interest in the message with or without changing or and appending related information to the message.
iv. **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 if accurate and the information required for the message is accesses quickly.
v. **Portability :** Email renders the physical location of the recipient and sender irrelevant. The email can be accessed fro any Personal computer equipped with the relevant communication hardware, software and link facilities.
vi. **Economical :** The advancements in communication technologies and competition among the communication service providers have made Email the most economical mode if sending messages. Since the speed of transmission is increasing, the time 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 n informal communication within the business enterprise.

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? (Marks6)

(b) What is the skill set expected from an IS Auditor? (Marks6)

(c) In Information Technology (Amended) Act 2008, what do Section 25 and Section 26 say about suspension of license to issue electronic signature certificate? (Marks4)

Answers:

(a) Any computerized environment is dependent on people. Though they play a critical role in success of an enterprise computing, it is a fact that threats always exist due to cyber crimes committed by people. The special skill sets of IT operational team, programmers; data administrator, etc. are key links in ensuring that the IT infrastructure delivers output as per user requirements. At

the same time, social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise. Threats also arise on account of dependence on external agencies. IT computing services are significantly dependant on various vendors and service providers for equipment supply and support; consumables, systems and program maintenance, air-conditioning, hot-site providers, utilities, etc. Following are some of the serious 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:*** *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. Denial of service 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.*
- ***Other:*** *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) IS Auditor's Role: In case, the auditor intends to carry out detailed reviews of, for example, logical design, it will probably be necessary either to employ expert assistance, or to undertake training in the particular technical skills required.

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

(a) Does system design follow a defined and acceptable standard?
(b) Are completed designs discussed and agreed with the users?
(c) Does the project's quality assurance procedure ensure that project documentation 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) Is auditors/security staffs invited to comment on the internal control aspects of system designs and development specifications?
(g) are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
(h) Are defects uncovered during quality reviews always corrected?

(i) Does the production of development specifications also include the production of relevant acceptance criteria?
(j) Has a configuration manger been appointed? Has the configuration management role been adequately defined?
(k) Are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?
(l) has sufficient IT been provided to assist with the configuration management task?
(m) Are effective procedures in place for recording, analyzing and reporting failures uncovered during testing?
(n) Are effective change management procedures are in place to control changes to configuration items?
(o) Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery?
(p) Has a system installation plan been developed and quality reviewed?
(q) Has an acceptance testing plan been drawn up? Is it to an acceptable standard? Does it cover all aspects of the user requirements specification?
(r) Does the acceptance test plan clearly allocate roles and responsibilities for undertaking and reviewing the results of acceptance testing?
(s) Has the acceptance test plan been discussed with, and signed off by the prospective system owner?
(t) Is the system development environment regularly backed up with copies of backed up configuration item held securely at a remote location?
(u) Has the development environment been recovered from backup media?
(v) Are contingency plans commensurate with the critically of the project.
(w) Do regular project board meetings take place to review project progress against budget and deadline?
(x) Is the Business Case regularly updated to ensure that the project remains viable.

(c) ***[Section 25] Suspension of License :***

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has -

a) made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;
b) failed to comply with the terms and conditions subject to which the license was granted;
c) failed to maintain the standards specified in Section 30 [Substituted for the words "under clause (b) of sub-section (2) of section 20;"]
d) contravened any provisions of this Act, rule, regulation or order made there under, revoke the license:

However,

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

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a license under sub-section (1), by order suspend such license pending the completion of any enquiry ordered by him:

However,

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.

(3) No Certifying Authority whose license has been suspended shall issue any Electronic Signature Certificate during such suspension.

[Section 26] Notice of suspension or revocation of license :

1) Where the license of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.
2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

However,
the data-base 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
However,
that the Controller may, if he considers necessary, publicize the contents of the data-base in such electronic or other media, as he may consider appropriate.

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? (Marks6)

(b) During the review of hardware, how will you review the change in the management controls? (Marks6)

(c) Describe the duties of certifying authority in respect of Digital Signature under Section 30 of Information Technology (Amended).Act 2008. (Marks4)

Answer:

(a)(i) Establishing Management Framework: This would include the following activities:

- Define information security policy;
- Define scope of ISMS including functional, asset, technical, and locational boundaries;
- Make appropriate risk assessment ;
- Identify areas of risk to be managed and degree of assurance required;
- Select appropriate controls;
- Prepare Statement of Applicability.

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

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

- Management control

· Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
· Procedure adopted to implement control under Implementation clause
· ISMS management procedure

· Document Control: The issues focused under this clause would be
- Ready availability
- Periodic review
- Maintain version control;
- Withdrawal when obsolete
- Preservation for legal purpose

· Records: The issues involved in record maintenance are as follows:
- Maintain to evidence compliance to Part 2 of BS7799.;
- Procedure for identifying, maintaining, retaining, and disposing of such evidence;
- Records to be legible, identifiable and traceable to activity involved.
- Storage to augment retrieval, and protection against damage.

(b) 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.

(c)Duties of Certifying Authority:

1. According to Section 30 of the Information Technology (Amendment) Act 2008, Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below:

- Make use of hardware, software and procedures that are secure from intrusion and misuse.
- Provide a reasonable level of reliability in its services, which are reasonably suited to the performance of intended functions.
- Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured and
- Observe such other standards, as specified by the regulation.

I. Every Certifying Authority shall ensure that every person employed by him complies with the provisions of the Act, or rules, regulations or orders made there under.

II. A Certifying Authority must display its licence at a conspicuous place of the premises in which it carries on its business. A Certifying Authority whose licence is suspended or revoked shall immediately surrender the license to the Controller.

III. Every Certifying Authority shall display its Digital Signature Certificate, which contains the public key corresponding to the private key used by that Certifying Authority and other relevant facts.

5. (a) Any system has to possess few key characteristics to qualify for a true Enterprise Resource Planning Solution. What are they? (Marks6)

(b) What are the characteristics of a good coded program? (Marks6)

(c) What are the points to be included when the documented audit program is developed? (Marks4)

Answer:

(a) ERP Characteristics: An ERP system is not only the integration of various organization processes, any system has to possess few key characteristics to qualify for a true ERP solution. These features are:

· **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 and 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) A good coded program should have the following characteristics:

· **Reliability:** It refers to the consistence which a program provides over a period of time. However poor setting of parameters and hard coding 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 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 take 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 **documented audit program** should include the following points (activities):

- Documentation of the IS auditor's procedures for collecting, analysing, interpreting, and documenting information during the audit.
- Objectives of the audit.
- Scope, nature, and degree of testing required achieving the audit objectives in each phase of the audit.
- Identification of technical aspects, risks, processes, and transactions which should be examined.

Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.

Working papers should record the audit plan, the nature, timing and extent of auditing procedures performed, and the conclusions drawn from the evidence obtained. All significant matters which require the exercise of judgment, together with the auditor's conclusion thereon, should be included in the working papers. The form and content of the working papers are affected by matters such as:

- The nature of the engagement
- The form of the auditor's report
- The nature and complexity of client's business
- The nature and condition of client's records and degree of reliance on internal controls.

In case of recurring audits, some working paper files may be classified as permanent audit files which are updated currently with information of continuing importance to succeeding audits, as distinct from the current audit files which contain information relating primarily to audit of a single period.

6. (a) What is the scope of IS Audit process? Explain the categories of IS Audit. (Marks6)

(b) What are the elements to be included in the methodology for the development of disaster recovery *me* business resumption plan? (Marks6)

(c)What are the goals of Business Continuity Plan? (Marks4)

Answers

(a) Scope of IS Audit The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluation, in the aggregate, provides 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 system, as under:

· Data
· Application systems
· Technology
· Facilities
· People

The information System auditor will consider whether the information obtained from the above reviews indicates coverage of the appropriate areas. The information system auditor will examine, among other, the following:

· Information system mission statement and agreed goals and objectives for information system activities.
· Assessment of the risks associated with the use of the information systems and approach to managing those risks.
· Information system strategy plans to implement the strategy and monitoring of progress against those plans.
· Information system budget and monitoring of variances.
· High level polices for information system use and the protection and monitoring of compliance with these polices.
· Major contract approval and monitoring of performance of the supplier.
· Monitoring of performance against service level agreements
· Acquisition of major systems and decisions on implementation.
· Impact of external influences on information system such as internet, merger of suppliers or liquidation etc.
· Control of self-assessment reports, internal and external audit reports, quality assurance reports or other reports on Information System.
· Business Continuity Planning, Testing thereof and Test results.
· Compliance with legal and regulatory requirements
· Appointment, performance monitoring and succession planning for senior information system staff including internal information system audit management and business process owners.

(b) Methodology and phases of developing a business continuity plan: 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 organization. The methodology emphasizes on the following:

· Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
· Obtaining commitment from appropriate management to support and participate in the effort;
· Defining recovery requirements from the perspective of business functions;
· Documenting the impact of an extended loss to operations and key business functions;
· Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;

· Selecting business continuity teams that ensure the proper balance required for plan development;
· Developing a business continuity plan that is understandable, easy to use and maintain; and
· 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.

(c) (i) The goals of the business continuity plan should be to:

· identify 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 effort.

(ii) A number of tasks are to be undertaken in this phase as enumerated under:

· Identify organizational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize potential threats that may lead to a disaster.
· Identify critical business processes.
· Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
· Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
· Determine the maximum allowable downtime for each business process.
· Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
· Determine the impact to the organization in the event of a disaster, e.g. financial reputation, etc.

7. Write short notes on any four of the following:

(a) Business Engineering. **(Marks4)**

(b) Constitution of Cyber Regulations Advisory Committee under Section 88 of Information Technology (Amended) Act 2008. **(Marks4)**

(c) Limitations of MIS. **(Marks4)**

(d) Basic ground rules for protecting computer held information system. **(Marks4)**

(e) Domains of COBIT. **(Marks4)**

Answers

(a) 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 the concept of Process Oriented Business Solutions enhanced by the client-server computing in

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 enterprise and customers. Information technology helps to develop business models, which assist in redesigning of business processes.

In short, Business Engineering is the method of development of business process according to changing requirements.

(b) ***[Section 88] Constitution of Advisory Committee:***

(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 travelling and other allowances as the Central Government may fix.

(c) Limitations of MIS: The main limitations of MIS are as follows:

- The quality of the outputs 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 making decisions in 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 time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision 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 types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in organizations, where the culture of hoarding information and not sharing with other holds.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

(d) We need to define a few basic ground rules that must be addressed sequentially:
· **Rule #1 :** We need to know that 'what the information systems are' and 'where these are located'.
· **Rule #2 :** We need 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 should and it become unavailable for whatever reason (loss, unauthorized modification, etc.)
These four rules are deceptively simple. For most organizations, providing answers to permit the design and implementation of any information system protection is very taxing.
(e) The four broad domains are identified: planning and organization, acquisition and implementation, delivery and support, and monitoring.

The high level control objectives for the **Planning and Organization domain**.

PO1	Defined Strategic IT Planned 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

The high level control objectives for the **Delivery and Support domain**.

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