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

Page No. of SHAYVIDZ Book : 2.20

Answer :

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

Page No. of SHAYVIDZ Book : 2.59

Answer :

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.

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

Page No. of SHAYVIDZ Book : 9.4

Answer:

ESTABLISHING BETTER INFORMATION PROTECTION

Steps the organisations need to take to keep the critical information protected:

i. Not All Data has the Same Value

- And, as such, the information may be handled and protected differently. Organizations must determine the value of the different types of information in their environment before they can plan for the appropriate levels of protection.

ii. Know Where the Critical Data Resides

- In today's business environment, this is normally the company's information systems infrastructure. Because each piece of information may require different levels of protection, identifying where each is located enables an organization to establish an integrated security solution.
- This approach also provides significant cost benefits, as the company does not need to spend more on protecting data than the data itself is worth.
- Protection solutions must be based on the most valuable information assets. The network environment also presents additional challenges for protecting information.

iii. Develop An Access Control Methodology

- Organizations must establish some type of access control methodology. For important data, this access control (and the associated auditing) should extend to the file level. Such access control extends from the host to the network. There are many types of solutions designed to provide this protected access.

iv. Protect Information Stored On Media

- Employees can cause considerable damage by walking out the door with information on floppy disks 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.

v. Review Hardcopy Output

- The hardcopy output of employees' daily work should also be reviewed. Although strategic plans in their final forms may be adequately protected, what measures are used to safeguard all drafts and working papers? What information is regularly placed in the recycle or trash containers without thought to its value?

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

Page No. of SHAYVIDZ Book : 3.51

Answer :

ACTIVITIES TO BE UNDERTAKEN

During a PIR, the team should, according to their terms of reference, review:

- The main functionality of the operational system against the User Requirements Specification
- System performance and operation
- The development techniques and methodologies employed
- Estimated time-scales and budgets, and identify reasons for variations
- Changes to requirements, and confirm that they were considered, authorised and implemented in accordance with change and configuration management standards
- Set out findings, conclusions and recommendations in a report for the authorizing authority to consider
- In addition to reviewing the functionality delivered by the new system, the review team will also need to look back to the Business Case on which the system was originally based to confirm that all the anticipated benefits, both tangible and intangible, have been delivered. It is also possible that the PIR will identify benefits that were not anticipated in the Business Case. These should be included in the PIR Report as additional justification for the investment, and to identify benefits that might be realized in other IS development projects. Following their deliberations on the PIR Report, the authorizing authority may either:
- endorse continuation of the system;
- approve plans to modify the system;
- terminate the system and make arrangements for a new course of action.

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 inter–related components of its Internal Control? Discuss them briefly.

Page No. of SHAYVIDZ Book : 3.3

Answer :

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

I. **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.

II. **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.

III. **Risk Assessment:** 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 cause material losses to an organisation.

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

V. **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.

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

Page No. of SHAYVIDZ Book : 1.31

Answer :

EXECUTIVE INFORMATION SYSTEMS (EIS)

An **Executive Information System (EIS)** is a type of management information system intended to facilitate and support the information and decision-making needs of senior executives by providing easy access to both internal and external information relevant to meeting the strategic goals of the organization. It is commonly considered as a specialized form of decision support system (DSS). The emphasis of EIS is on graphical displays and easy-to-use user interfaces. They offer strong reporting and drill-down capabilities. In general, EIS are enterprise-wide DSS that help top-level executives analyze, compare, and highlight trends in important variables so that they can monitor performance and identify opportunities and problems. EIS and data warehousing technologies are converging in the marketplace.

Characteristics of EIS

- EIS is a Computer-based-information system that serves the information need 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 tool like trend analysis, market conditions etc.
- EIS can easily be given a DSS support for decision making.
- EIS is easily connected to internet.
- User Friendly
- Information tends to be presented by pictorial and graphical means.

- Information is presented in summary format.
- The ability to manipulate data, to project what if analysis and to work with modeling tool within the system.

(c) Explain any four features of Electronic Mail.

Page No. of SHAYVIDZ Book : 1.39

Answer :

Electronic Mail: Various features of electronic mail are stated below :

- **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 use of paper 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 branches of a bank using Email resulting in a lot of saving of paper. 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 irrelevant. 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 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 for 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?

Page No. of SHAYVIDZ Book : 5.6

Answer :

THREATS DUE TO CYBER CRIMES

i. *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.

ii. *Fraud :*

It occurs on account of intentional 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.

iii. *Theft of proprietary information :*

It is the illegal obtaining 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.

iv. *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 those results 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.

v. *Vandalism or sabotage :*

It is the deliberate or malicious, damage, defacement, destruction or other alteration of electronic files, data, web pages, and programs.

vi. *Computer virus :*

A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user.

vii. *Other :*

Threat includes several other cases such as intrusions, 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) What is the skill set expected from an IS Auditor?

Page No. of SHAYVIDZ Book : 3.7

Answer :

The **SET OF SKILLS** that is generally expected of an IS auditor include :

- **Sound knowledge** of business operations, practices and compliance requirements,
- Should possess the requisite professional **technical qualification and certifications,**
- A good **understanding of information Risks and Controls,**
- **Knowledge of IT strategies, policy and procedure controls,**
- Good **knowledge of Professional Standards and Best practices** of IT controls and security, and
- **Ability to understand technical and manual controls** relating to business continuity.

Therefore the audit process begins by defining the scope and objectives to adapt the standards and benchmarks for developing information model for collecting and evaluating evidence to execute the audit.

(c) In Information Technology (Amended) Act, 2008, what do Section 25 and Section 26 say about Suspension of License to issue Electronic Signature Certificate?

Page No. of SHAYVIDZ Book : 10.16

Answer :

Sec 25 Suspension of License

- The Controller may, if he is satisfied **after making such inquiry**, as he may think fit, that a Certifying Authority has -
  - ✓ 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;
  - ✓ failed to comply with the terms and conditions subject to which the license was granted;
  - ✓ failed to maintain the standards specified in Section 30
  - ✓ Contravened any provisions of this Act, rule, regulation or order made there under,

  revoke the license. **(But before revocation, Reasonable Opportunity of being heard is necessary.)**
- The Controller may, if he has **reasonable cause to believe** that there is **any ground** for revoking a license, by order, **suspend** such license pending the completion of any enquiry ordered by him. ***However***, no license shall be suspended for a period **exceeding 10 Days** unless Certifying Authority has been given a **reasonable opportunity** of showing cause against the proposed suspension.
- No Certifying Authority whose license has been suspended shall issue any Electronic Signature Certificate during such suspension.

Sec 26 Notice of suspension or revocation of license

- Where the license of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, **in the database maintained by him / official gazette.**

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?

Page No. of SHAYVIDZ Book : 8.7

Answer :

Access Control

Access to information and business processes should be controlled on the business and security requirements.

This will include defining access control policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication, node authentication, segregation of networks, network connection control, network routing control, operating system access control, user identification and authentication, use of system utilities, application access control, monitoring system access and use and ensuring information security when using mobile computing and tele-working facilities.

The detailed control and objectives thereof are as follows:

- ***Business requirement for access control***
  To control access to information.
- ***User access management***
  To prevent unauthorised access to info systems.
- ***User responsibilities***
  To prevent unauthorised user access.
- ***Network access control***
  Protection of networked services.
- ***Operating system access control***
  To prevent unauthorised computer access.
- ***Application Access Control***
  To prevent unauthorised access to information held in information systems.
- ***Monitoring System Access and use***
  To detect unauthorised activities.
- ***Mobile Computing and teleworking***
  To ensure information security when using mobile computing and teleworking facilities.

(b) During the review of hardware, how will you review the change in the Management Controls?

ICAI Study Material – Page No. 4.25

Review the change in management controls for the following:

- Determine if changes to hardware configuration are planned and timely information is given to the individual 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 changes in 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 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 of all hardware changes to ensure that changes are coordinated properly.

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

Page No. of SHAYVIDZ Book : 10.18

Answer :

Sec 30 Duties of Certifying Authorities (Standards to be followed)

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

- make **use of hardware, software, and procedures** that are secure from intrusion and misuse
- provide a **reasonable level of reliability** in its services which arc reasonably suited to the performance of intended functions;
- adhere to **security procedures** to ensure that the secrecy and privacy of the Electronic Signature are assured
  - ✓ be the repository of all Electronic Signature Certificates issued under this Act
  - ✓ publish information regarding its practices, Electronic Signature Certificates and current status of such certificates
- observe such other standards as may be specified by regulations

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

Page No. of SHAYVIDZ Book : 7.4

Answer :

Characteristic of ERP

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:

1. 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).

2. Modular & Open

ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.

3. Comprehensive

It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

4. 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.

5. 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 organisation.

6. New Technology

It should incorporate cutting-edge and future-proof technologies such as object orientation into product development and ensure inter-operability with the Internet and other emerging technologies.

(b) What are the characteristics of a Good Coded Program?

Page No. of SHAYVIDZ Book : 2.46

Answer :

CHARACTERISTICS OF A GOOD CODED PROGRAM

- **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) What are the points to be included when the documented audit program is developed?

Page No. of SHAYVIDZ Book : 9.22

Answer :

I. PLANNING THE DOCUMENTATION

Parameters that are required to be considered for planning documentation

1. The importance of planning and understanding the planning process requires identifying three planning questions:

   Knowing Your Resources

   The three basic resources: time, people, money. One has to check for their availability and affordability.

   Defining the Scope and Audience

   The same report may undergo significant changes depending on the character of report and nature of audience. Presentation on Balance Sheet made to bankers and to investors would be quite different in content and focus.

   Using a Scope Definition Report

   It is critical to know how to complete a Scope Definition Report. This report helps in developing a workable schedule for completing the project.

2. The Documentation Writer: The qualities and skills that the documentation writer would need. The requirement may often be legal in nature.
3. Rules to guide documentation writing: The four steps of writing documentation described in subsequent section.

II. GATHERING INFORMATION

To be able to have a good documentation, it is necessary to get information about the reader and the requirement of the document.

- ***About the Reader:*** Finding information about the reader by doing a task analysis. Three parts of the task: viz. input, process, output will have to be identified before one could develop an understanding of a reader.

- ***About the Subject:*** The three sources of information about a subject are people, paper, and the object of the report.

III. ORGANIZING INFORMATION

Organizing information involves deciding what information to include and how to sequence it. This covers five organizational sequences and examines how to divide the documentation into various sections and subsections.

- ***Selecting Information***: Selecting 'what the reader needs to know'. Organizing the information into a useful sequence.
- ***Organizing the Documentation***: Using the five organizational sequences: subject, difficulty, chronological, importance and analytical.
- ***Dividing Into Sections***: Dividing documentation into chapters or sections.
- ***Dividing Into Subsections***: Dividing sections or chapters into subsections.

IV. WRITING THE DOCUMENTATION

Writing is governed by the following major rules/principles:

- ***Writing in Active Voice***: Using active voice in documentation.
- ***Giving the Consequences***: Giving the consequences of the reader's action.
- ***Writing from General to Specific***: Designing the documentation from general to specific.
- ***Consistency***: Using style, order and format consistently.
- ***Writing Online Documentation***: Laying down guidelines for writing online documentation. Using appropriate techniques to emphasize text.

V. FINALIZING DOCUMENTS

This section identifies the tasks involved in reviewing and testing the document, generating the glossary and index and formatting the document for final production.

• **Reviewing and Testing**

Selection of reviewer of the documentation involves identification of subject and communication skill. The reviewer must be provided with adequate information regarding the audience and object of the report. In order to ensure objectivity It is recommended that the reviewer be a person who has not been involved in the documentation process.

• **Generating the Glossary and Index**

Compilation of a glossary and generation of an index are two major tasks for a complete documentation. In order to achieve this task it is necessary to mark the Index and glossary entries at the stage of documentation itself. Word processing software comes with an inbuilt ability of creating an index from the identified text in the body of the document.

• **Formatting and Production**

The idea of creating a good document is incomprehensible without first deciding on a good design for the same. This involves choosing effective formatting options for headings, subheadings, section breaks, formatting, and allied. It also important to select an appropriate binding style that would aid filing and ease of consultation.

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

Page No. of SHAYVIDZ Book : 3.7 & 3.8

Answer :

The Audit of an IS environment to evaluate the systems, practices and operations may include one or both of the following :

- Assessment of internal controls within the IS environment to assure validity, reliability, and security information.
- Assessment of the efficiency and effectiveness of the IS environment in economic terms.

CATEGORIES OF IS AUDITS

IT audits has been categorized into five types:

I. **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.

II. **Information Processing Facilities:** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

III. **Systems and Applications:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

IV. **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.

V. **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) What are the elements to be included in the methodology for the development of Disaster Recovery / Business Resumption Plan?

Page No. of SHAYVIDZ Book : 6.4

Answer :

DEVELOPING A BUSINESS CONTINUITY PLAN

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;

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) What are the goals of Business Continuity Plan?

Page No. of SHAYVIDZ Book : 6.3

Answer :

GOALS OF THE BUSINESS CONTINUITY PLAN should be to:

I. **Identify weaknesses** and implement a disaster prevention program;
II. **Minimise the duration** of a serious disruption to business operations;
III. Facilitate effective **co-ordination of recovery tasks**; and
IV. **Reduce the complexity** of the recovery effort.

7. (a) Business Engineering.

Page No. of SHAYVIDZ Book : 7.10

Answer :

Business Engineering (= Information Technology + 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.
- Business Engineering is the method of development of business processes according to changing requirements.

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

Page No. of SHAYVIDZ Book : 10.41

Answer :

Sec 88 Constitution of Advisory Committee

- The Central Government shall constitute a Committee called the Cyber Regulations Advisory Committee.
- 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.
- The Cyber Regulations Advisory Committee **shall advise** -
  - ✓ **the Central Government** either generally as regards any rules or for any other purpose connected with this Act;
  - ✓ **the Controller** in framing the regulations under this Act.
- Travelling & other allowances to non-official members shall be paid as fixed by the central government.

(c) Limitations of MIS.

Page No. of SHAYVIDZ Book : 1.22

Answer :

Limitations of the Management Information System

1. Depends upon Quality of input:

The quality of the outputs of MIS is basically governed by the quantity of input and processes.

2. Not a Substitute of Management:

MIS is not a substitute for effective management which 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.

3. Can't give Ad-hoc Reports:

MIS gives exceptional report, mathematical report but can't give Ad-hoc (unplanned, unprepared, informal) reports. MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.

4. Doesn't consider Non-Quantitative Factors:

MIS takes into account mainly quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives.

5. Less useful for Unstructured Decision:

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.

6. Holding information & not sharing:

The effectiveness of MIS is reduced in organizations, where the culture of holding information and not sharing with other.

7. Top Management Change:

MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

8. Limitation of TPS:

MIS is constrained by the limitation of TPS.

9. Lack of tight integration:

MIS prepares for various functions like Finance, Marketing, Production, HR but MIS lacks at tight integration.

10. Only Internal Data:

MIS generates information based on internal data and not on external data.

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

Page No. of SHAYVIDZ Book : 9.5

Answer :

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 it become unavailable for whatever reason (loss, unauthorized modification, etc.)"

(e) Domains of COBIT.

Page No. of SHAYVIDZ Book : 8.16

Answer :

COBIT STRUCTURE

COBIT covers four domains which are given as follows:

i. Plan and Organize
ii. Acquire and Implement
iii. Deliver and Support
iv. Monitor and Evaluate

I. Plan and Organize

The Plan and Organize domain covers the use of information & technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructure form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT.

II. 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 adopt in order to prolong the life of an IT system and its components.

III. Deliver and Support

The Deliver and Support domain focuses on the delivery aspects of the information technology. 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.

IV. 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 business objectives and the company's control processes by internal and external auditors.

Chapter No.	Chapter Name	Ques No.	Marks	Total Marks
1	Information Systems Concepts	2(b) 2(c) 7(c)	6 4 4	**14**
2	System Development Life Cycle Methodology	1(a) 1(b) 5(b)	5 5 6	**16**
3	Control Objectives	1(d) 2(a) 3(b) 6(a)	5 6 6 6	**23**
4	Testing – General and Automated Control	4(b)	6	**6**
5	Risk Assessment Methodologies and Applications	3(a)	6	**6**
6	Business Continuity Planning and Disaster Recovery Planning	6(b) 6(c)	6 4	**10**
7	An Overview of Enterprise Resource Planning (ERP)	5(a) 7(a)	6 4	**10**
8	Information Systems Auditing Standards, Guidelines, Best Practices	4(a) 7(e)	6 4	**10**
9	Drafting of IS Policy, Audit Policy, IS Audit Reporting – A Practical Perspective	1(c) 5(c) 7(d)	5 4 4	**13**
10	Information Technology (Amendment) Act, 2008	3(c) 4(c) 7(b)	4 4 4	**12**
Total				**120**