PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Information Systems Concepts

1. (a) Discuss the characteristics of Computer based Information Systems.

   (b) Explain the main limitations of a Management Information System (MIS).

2. Describe a practical set of principles to guide the design of measures and indicators to be included in an Executive Information System (EIS).

Software Development Life Cycle Methodology

3. Why organizations fail to achieve their systems development objectives; explain in brief.

4. (a) Discuss the weaknesses of Rapid Application Development (RAD) approach.

   (b) 'While eliciting information to delineate the scope, few aspects need to be kept in mind during the preliminary investigation of the development life cycle'. Explain these aspects, in brief.

5. (a) 'Management should establish acquisition standards that address the same security and reliability issues as development standards'. What are the areas that need to be focused by Acquisition Standards?

   (b) Discuss the major characteristics of a good coded program.

Control Objectives

6. (a) Discuss the interrelated components of internal controls used within an organization.

   (b) Explain the set of skills that is generally expected from an IS Auditor.

7. Discuss major controlling techniques/ways for remote and distributed data processing applications.

8. (a) What are the points that should be kept in mind by an IS Auditor while working with logical access control mechanism?

   (b) What are the aspects that should be evaluated by an IS Auditor while reviewing the adequacy of data security controls?

Testing – General and Automated Controls

9. (a) Describe the advantages of Continuous Auditing Techniques in brief.

   (b) Discuss three phases of Information System Controls Audit in brief.

Risk Assessment Methodologies and Applications

10. (a) Explain the threats due to cyber crimes.

(b) Briefly explain the risk management process.

Business Continuity Planning and Disaster Recovery Planning

11. (a) What are the tasks that should be undertaken in 'Business Impact Analysis'? Explain in brief.

    (b) Explain the objectives of performing BCP tests.

An Overview of Enterprise Resource Planning (ERP)

12. (a) Discuss the guidelines, which are to be followed before starting the implementation of an ERP Package.

    (b) Discuss any five benefits achieved by implementing an ERP package.

Information Systems Auditing Standards, Guidelines, Best Practices

13. (a) What are the issues that should be covered by a security policy? Explain in brief.

    (b) Discus controls and objectives of access control.

14. Discuss 'Acquire and Implement' and 'Deliver and Support' domains of COBIT.

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

15. Explain the major points, which need to be taken into account for the proper implementation of Physical and Environmental Security.

Information Technology (Amendment) Act 2008

16. (a) Discuss Section 19 relating to the recognition of foreign Certifying Authorities under Information Technology (Amendment) Act, 2008.

    (b) Describe "license to issue electronic signature certificates" with respect to the Section 21 of Information Technology (Amendment) Act, 2008.

17. Discuss "Appeal to Cyber Regulations Appellate Tribunal" under Section 57 of Information Technology (Amendment) Act, 2008.

Questions based on Short Notes

18. Write short notes on the following:

    (a) Worms

    (b) Corrective and Adaptive Maintenance

    (c) Time Bomb and Logic Bomb

19. Write short notes on the following:

    (a) Scoring Approach for risk evaluation

    (b) Recovery Plan

(c) Differential Backup

20. Write short notes on the following:

(a) Reasons for failure of ERP projects

(b) Configuration Management under IT Infrastructure Library (ITIL)

(c) Powers of State Government to make rules in Section 90 of Information Technology (Amendment) Act, 2008

Questions based on Case Studies

21. ABC Technologies Ltd. deals with the software developments for various domains. The company is following SDLC best practices for its different activities. For any software to be developed, after possible solutions are identified, project feasibility i.e. the likelihood that the system will be useful for the organization, is determined. After this, other stages of the SDLC are followed with their best practices. A system development methodology is a formalized, standardized and documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations.

Read the above carefully and answer the following:

(a) What is a feasibility study? Explain the dimensions under which the feasibility study of a system is evaluated.

(b) For the development of software, various techniques/models are used e.g. waterfall, incremental, spiral etc; in which, each has some strengths and some weaknesses. Discuss the weaknesses of the incremental model.

(c) What do you mean by cohesion and coupling with reference to the software designing.

22. Tremendous use of Information Technology in a large number of organizations has made it imperative that appropriate information systems are implemented in the organizations. Information technology covers all key aspects of business processes of an enterprise and has an impact on its strategic and competitive advantage for its success. The enterprise strategy outlines the approach, it wishes to formulate with relevant policies and procedures on harnessing the resources to achieve business objectives. Controls are designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

Read the above carefully and answer the following:

(a) Explain the activities of IS Control Audit process in brief.

(b) What is an Intrusion detection? Explain two broad categories of intrusion detection systems in brief.

(c) Briefly discuss auditors' role in the change management process.

23. PQR Enterprises is a leading company in the manufacturing of baby toys. The company is in the process of automation of its various business processes. During this automation, technical consultant of the company suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risks. A risk is the likelihood that an organization would face, if vulnerability is exploited or a threat becoming harmful. Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. This means, there are new risk areas that could have a significant impact on critical business operations, such as, external dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information; growing potential for misuse and abuse of information system affecting privacy and ethical values; and increasing requirements for availability and robustness.

    Read the above carefully and answer the following:

    (a) Define vulnerability, likelihood and attack with the help of suitable examples.

    (b) Write two primary questions, which should be considered while evaluating the risk inherent in a business function.

    (c) In automation of the business modules, authentication of electronic records is an important activity. How Information Technology (Amendment) Act 2008 addresses this issue with reference to its Section 3?

24. XYZ Consultants is a leading company, which provides various consultancy services to the organizations worldwide for different activities of their business modules. Recently, the company has taken a project for the automation of various business modules of a government organization to improve the overall e-governance system. There are around 50 modules for which the complete automation is to be done. It involves a number of activities starting from the capturing of the requirements to the maintenance. The users/officials of the organization are not well versed with technically identifying and reporting of their requirements. Hence, various brainstorming sessions have been organized so many times along with personal interactions; this resulted in better identification of requirements. Further, Business continuity and disaster recovery planning are two key activities in this entire process, which must be taken care *right from the beginning*. Business continuity focuses on maintaining the operations of an organization, especially the IT infrastructure in face of a threat that has materialized. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operations using a prioritized resumption list.

© The Institute of Chartered Accountants of India

Read the above carefully and answer the following:

(a) Discuss any two fact finding techniques with reference to requirements phase of SDLC?

(b) What should be the goals of a Business continuity plan? Explain in brief.

(c) Discuss major backup tips in brief.

25. ABC Ltd is a global BPO offering financial and accounting services to customers across the globe. It primarily caters to the back office accounting requirements of its parent company based in US with operations in India, SriLanka, South Africa, China, Malaysia, Singapore and Mauritius. The company provides outsourced financial services such as general bookkeeping and specific accounting area support (accounts payable, accounts receivable, general ledger) to multiple legal entities across the globe. Having established its success in managing the accounting requirements of the highly distributed branch office network of its parent company, the company is all set to expand its scope of operations to offer similar services to other clients as well on 24×7 basis. For this, the company is in the process of implementing a globally recognized ERP solution, which could meet the requirements of the customers and fit into the business processes. The company requires a robust, secure and flexible solution that could unify its bifurcated process and help them to achieve greater operational efficiency.

Read the above carefully and answer the following:

(a) ‘Many post-implementation problems from an ERP solution occur due to wrong expectations and fears. Explain some popular expectations in brief.

(b) What is Change Control Process with respect to system development? Also explain its associated risks.

(c) Describe the controls and objectives of System Development and Maintenance in brief.

SUGGESTED ANSWERS / HINTS

1. (a) Major characteristics of Computer Based Information Systems are as follows:

- All systems work for predetermined objectives and the system is designed and developed accordingly.
- In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
- If one subsystem or component of a system fails, in most of the cases the whole system does not work. However, it depends on how the subsystems are

interrelated.

- The way, a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system.
- The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.

(b) Main limitations of a Management Information System (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, 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.
- 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 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.

2. A practical set of principles to guide the design of measures and indicators to be included in an EIS are given as follows:

- EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as a part of the process of work. An EIS should not add substantially to the workload of managers or staff.
- EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service.

© The Institute of Chartered Accountants of India

- Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers.
- EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff; people must feel that they, as individuals, can contribute to improving the performance of the organization.
- EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential should not be part of the EIS or the management system of the organization.
- EIS measures must evolve to meet the changing needs of the organization.

3. There are many reasons, which are responsible for failure of organizations to achieve their systems development objectives. Some of them are given as follows:

   - **Lack of senior management support and involvement in information systems development:** Developers and users of information systems watch senior management to determine which systems development projects are important and act accordingly by shifting their efforts away from any project which is not receiving management attention. In addition, management can see that adequate resources, as well as budgetary control over use of those resources, are dedicated to the project.
   - **Shifting user needs:** User requirements for information technology are constantly changing. As these changes accelerate, there will be more requests for systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purposes might change since the development process began.
   - **New technologies**: When an organization tries to create a competitive advantage by applying advance Information technology, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the technology.
   - **Lack of standard project management and systems development methodologies:** Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
   - **Overworked or under-trained development staff:** In many cases, systems developers often lack sufficient education background. Furthermore, many

companies do little to help their development personnel stay technically sound. Currently in these organizations, a training plan and training budget do not exist.

- Resistance to change: People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project is doomed to failure.
- Lack of user participation: Users must participate in the development effort to define their requirements, feel ownership for project success, and work to resolve development problems. User participation also helps reduce user resistance to change.
- Inadequate testing and user training: New systems must be tested before installation to determine that they operate correctly. Users must be trained to effectively utilize the new system.

To overcome these and other problems, organizations must execute the systems development process efficiently and effectively.

4. (a) Major weaknesses of RAD are given as follows:

- More speed and lower cost may lead to a lower overall system quality.
- There is a danger of misalignment of developed system with the business due to missing information.
- Project may end up with more requirements than needed (gold-plating).
- Potential for feature creep where more and more features are added to the system over the course of development exist.
- Potential for inconsistent designs within and across systems is there.
- Potential for violation of programming standards related to inconsistent naming conventions and inconsistent documentation exists,
- Difficulty with module reuse for future systems is also there.
- Potential for designed system to lack scalability may be there.
- Potential for lack of attention to later system administration needs built into system.
- High cost of commitment on the part if key user personnel exist.
- Formal reviews and audits are more difficult to implement than for a complete system.
- Tendency for difficult problems to be pushed to the future to demonstrate early success to management may be there.

© The Institute of Chartered Accountants of India

- Since some modules will be completed much earlier than others, well –defined interfaces are required.

(b) While eliciting information to delineate the scope, various aspects that need to be kept in mind during the preliminary investigation of the development life cycle are discussed below:

- Different users will represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project alternately called champion or executive sponsor of the project, addressing his concerns should be the basis of the scope.
- While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
- While presenting the proposed solution for a problem, the development organization has to clearly quantify the economic benefits to the user organization. The information required has to be gathered at this stage. For example - when a system is proposed for Road tax collection, data on the extent of collection and defaults is required to quantify benefits that will result to the Transport Department.
- It is also necessary to understand the impact of the solution on the organization- its structure, roles and responsibilities. Solutions which have a wide impact are likely to meet with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle this have had a very poor ERP implementation record, with disastrous consequences.
- While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weight-age too. These factors have to be considered from the perspective of the user management and resolved. For example- in a security system, how foolproof it is, may be a critical a factor like the economic benefits that entail.

5. (a) Acquisition standards should focus on the following areas:

- Ensuring security, reliability, and functionality already built into a product.
- Ensuring managers complete appropriate vendor, contract, and licensing reviews and acquiring products compatible with existing systems.
- Including invitations-to-tender and request-for-proposals. Invitations-to-tender involve soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software. Request-for-proposals involve soliciting bids when acquiring off-the-shelf or third-party developed software.

© The Institute of Chartered Accountants of India

- Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.

(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.

6. (a) Internal controls used within an organization 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 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 organization.
- 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.

© The Institute of Chartered Accountants of India

- **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) The set of skills that is generally expected from an IS auditor, includes:

- Sound knowledge of business operations, practices and compliance requirements,
- Should possess the requisite professional technical qualification and certifications,
- An good understanding of information Risks and Controls,
- Knowledge of IT strategies, policy 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.

7. Remote and distributed data processing applications can be controlled by the following techniques/ways:

- Remote access to computer and data files through the network should be implemented.
- Having a terminal lock can assure physical security to some extent.
- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
- In order to prevent the unauthorized users gain entry into the system, there should be proper control mechanisms over system documentation and manuals.
- Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
- When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.

8. (a) An IS auditor should keep the following points in mind while working with logical access control mechanisms:

- Reviewing the relevant documents pertaining go logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system.
- The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency.
- Deficiencies or redundancies must be identified and evaluated.
- By supplying appropriate audit techniques, he must be in a position to verify test controls over access paths to determine its effective functioning.
- He has to evaluate the access control mechanism, analyze the test results and other auditing evidences and verify whether the control objectives have been achieved.
- The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.

(b) An IS auditor is responsible to evaluate the following aspects when reviewing the adequacy of data security controls:

- Who is responsible for the accuracy of the data?
- Who is permitted to update data?
- Who is permitted to read and use the data?
- Who is responsible for determining who can read and update the data?
- Who controls the security of the data?
- If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
- Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
- The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

9. (a) Some of the advantages of Continuous Audit Techniques are as under:

- Timely, comprehensive and detailed auditing – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- Surprise test capability – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.

© The Institute of Chartered Accountants of India

- Information to system staff on meeting of objectives - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- Training for new users – Using the ITFs new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

(b) The Information System (IS) controls audit involves the following three phases:

- Planning: The auditor determines an effective and efficient way to obtain the evidential matter necessary to achieve the objectives of the IS controls audit and the audit report. For financial audits, the auditor develops an audit strategy and an audit plan. For performance audits, the auditor develops an audit plan.
- Testing: The auditor tests the effectiveness of IS controls that are relevant to the audit objectives.
- Reporting: The auditor concludes on the effect of any identified IS control weaknesses with respect to the audit objectives and reports the results of the audit, including any material weaknesses and other significant deficiencies.

10. (a) Major threats due to cyber crimes are given below:

- 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 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.
- 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.
- 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.
- 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: A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user.
- Others: 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) Risk Management Process : The broad process of risk management will be as follows:

- Identify the technology related risks under the scope of operational risks.
- Assess the identified risks in terms of probability and exposure.
- Classify the risks as systematic and unsystematic.
- Identify various managerial actions that can reduce exposure to systematic risks and the cost of implementing the same.
- Look out for technological solutions available to mitigate unsystematic risks
- Identify the contribution of the technology in reducing the overall risk exposure. The analysis should not be restricted to the instant area of application of the technology but should be extended across the entire organization. This is necessary since many technologies may mitigate a specific type of risk but can introduce other kinds of risks.
- Evaluate the technology risk premium on the available solutions and compare the same with the possible value of loss from the exposure.
- Match the analysis with the management policy on risk appetite and decide on induction of the same.

11. (a) The tasks that should be undertaken in ‘Business Impact Analysis’ are given as 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.

© The Institute of Chartered Accountants of India

- Determine the impact to the organization in the event of a disaster, e.g. financial reputation, etc.

(b) The objectives of performing BCP tests are to ensure that

- the recovery procedures are complete and workable;
- the competence of personnel in their performance of recovery procedures can be evaluated;
- the resources such as business processes, IS systems, personnel, facilities and data are obtainable and operational to perform recovery processes;
- the manual recovery procedures and IT backup system/s are current and can either be operational or restored and
- the success or failure of the business continuity training program is monitored.

12. (a) The guidelines, which are to be followed before starting the implementation of an ERP package, are given as follows.

- Understanding the corporate needs and culture of the organization and then adopt the implementation technique to match these factors.
- Doing a business process redesign exercise prior to starting the implementation.
- Establishing a good communication network across the organization.
- Providing a strong and effective leadership so that people down the line are well motivated.
- Finding an efficient and capable project manager.
- Creating a balanced team of implementation consultants who can work together as a team.
- Selecting a good implementation methodology with minimum customization.
- Training end users.
- Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

(b) Five benefits achieved by implementing the ERP packages are given as follows:

- Gives Accounts Payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations;
- Reduce paper documents by providing on-line formats for quickly entering and retrieving information;

© The Institute of Chartered Accountants of India

- Improves timeliness of information by permitting posting daily instead of monthly;
- Greater accuracy of information with detailed content, better presentation, satisfactory for the auditors; and
- Better monitoring and quicker resolution of queries.

13. (a) A security policy should cover the following issues:

- a definition of information security,
- a statement of management intention supporting the goals and principles of information security,
- allocation of responsibilities for every aspect of implementation,
- an explanation of specific applicable proprietary and general, principles, standards and compliance requirements,
- an explanation of the process for reporting of suspected security incidents,
- a defined review process for maintaining the policy document,
- means for assessing the effectiveness of the policy embracing cost and technological changes, and
- nomination of the policy owner.

(b) The detailed controls and objectives of access controls are as follows:

- *Business requirement for access control* : To control access to information;
- *User access management* : To prevent unauthorized access to info 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.

14. ‘Acquire and Implement’ domain of COBIT: 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

© The Institute of Chartered Accountants of India

system and its components. The following table lists the IT processes contained in the Acquire and Implement domain.

IT PROCESSES

Acquire and Implement

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

'Deliver and Support' domain of COBIT: 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. The following table lists the IT processes contained in the Deliver and Support domain.

IT PROCESSES

Deliver and Support

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

© The Institute of Chartered Accountants of India

DS12 Manage the Physical Environment
DS13 Manage Operations

15. For the proper implementation of Physical and Environment Security, the following points need to taken into account:

- Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
- The IT infrastructure must be physically protected.
- Access to secure areas must remain limited to authorized staff only.
- Confidential and sensitive information and valuable assets must always be securely locked away when not in use.
- Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to systems.
- Supplies and equipment must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities.
- Equipment, information or software must not be taken off-site without proper authorization.
- Wherever practical, premises housing computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.
- The location of the equipment room(s) must not be obvious. It will also where practical be located away from, and protected against threats of, unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

16. (a) [Section 19] Recognition of foreign Certifying Authorities :

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognized under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub- section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

© The Institute of Chartered Accountants of India

(b) [Section 21] License to issue electronic signature certificates:

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a license to issue Electronic Signature Certificates.

(2) No license shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Electronic Signature Certificates as may be prescribed by the Central Government.

(3) A license granted under this section shall -

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

17. [Section 57] Appeal to Cyber Regulations Appellate Tribunal:

(1) Save as provided in sub-section (2), any person aggrieved by an order made by a Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

However,

the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

© The Institute of Chartered Accountants of India

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

18. (a) Worms : A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses. Worms can help to sabotage systems yet they can also be used to perform some useful tasks. For example, worms can be used in the installation of a network. A worm can be inserted in a network and we can check for its presence at each node. A node, which does not indicate the presence of the worm for quite some time, can be assumed as not connected to the network.

Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive. Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

(b) Corrective maintenance: Corrective maintenance deals with fixing bugs in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.

Adaptive maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.

(c) Time Bomb: This name has been borrowed from its physical counterpart because of mechanism of activation. A physical time bomb explodes at the time it is set for (unless somebody forces it to explode early), like wise the computer time bomb causes a perverse activity, such as, disruption of computer system, modifications, or destructions of stored information etc. on a particular date and time for which it has been developed. The computer clock initiates it.

Logic Bomb: They resemble time bombs in their destruction activity. Logic bombs are activated by combination of events. For example, a code like; “If a file named DELETENOT is deleted then destroy the memory contents by writing ones.” This code segment, on execution, may cause destruction of the contents of the memory

© The Institute of Chartered Accountants of India

on deleting a file named DELETENOT. These bombs can be set to go off at a future time or event.

19. (a) Scoring Approach for risk evaluation: In the Scoring approach, the risks in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.

(b) Recovery Plan: The backup plan is intended to restore operations quickly so the information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plans should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of a recovery committee must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

(c) Differential Backup: A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved. Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

20. (a) Reasons for failure of ERP projects

At its simplest level, ERP is a set of best practices for performing the various duties in the departments of your company, including in finance, manufacturing and the warehouse. To get the most from the software, you have to get people inside your company to adopt the work methods outlined in the software. If the people in the different departments that will use ERP don't agree that the work methods embedded in the software are better than the ones they currently use, they will resist using the software or will want IT to change the software to match the ways they currently do things. This is where ERP projects break down.

Political fights erupt over how or even whether the software will be installed. IT gets bogged down in long, expensive customization efforts to modify the ERP software to fit with powerful business barons' wishes. Customizations make the software more unstable and harder to maintain when it finally does come to life. Because ERP covers so much of what a business does, a failure in the software can bring a company to a halt, literally.

The mistake companies make is assuming that changing people's habits will be easier than customizing the software. It's not. Getting people inside your company to use the software to improve the ways they do their jobs is by far the harder challenge. If people are resistant to change, then the ERP project is more likely to fail.

(b) Configuration Management in ITIL: Configuration Management is a process that tracks all of the individual Configuration Items (CI) in a system. A system may be as simple as a single server, or as complex as the entire IT department. Configuration Management includes:

- Creating a parts list of every CI (hardware or software) in the system.
- Defining the relationship of CIs in the system
- Tracking of the status of each CI, both its current status and its history.
- Tracking all Requests for Change to the system.
- Verifying and ensuring that the CI parts list is complete and correct.

There are five basic activities in configuration management:

- Planning
- Identification
- Control
- Status accounting
- Verification and Audit

(c) [Section 90] Power of State Government to make rules:

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely

(a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;

© The Institute of Chartered Accountants of India

(b) for matters specified in sub-section (2) of section 6;

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.

21. (a) A feasibility study is carried out by the system analysts. It refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. The Feasibility Study of a system is evaluated under following dimensions:

- *Technical:* Is the technology needed available?
- *Financial:* Is the solution viable financially?
- *Economic*: Return on Investment?
- *Schedule/Time*: Can the system be delivered on time?
- *Resources*: Are human resources reluctant for the solution?
- *Operational*: How will the solution work?
- *Behavioral*: Is the solution going to bring any adverse effect on quality of work life?
- *Legal*: Is the solution valid in legal terms?

(b) Major weaknesses of the incremental model are given as follows:

- When utilizing a series of mini-waterfalls for a small part of the system before moving onto the next increment, there is usually a lack of overall consideration of the business problem and technical requirements for the overall system.
- Each phase of an iteration is rigid and do not overlap each other.
- Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.
- Since some modules will be completed much earlier than others, well-defined interfaces are required.
- Difficult problems tend to be purchased to the future to demonstrate early success to management.

(c) A module is a manageable unit containing data and instructions to perform a well-defined task. Interaction among modules is based on well-defined interfaces. Modularity is measured by two parameters: Cohesion and Coupling.

Cohesion refers to the manner in which elements within a module are linked.

Coupling is a measure of the interconnection between modules. It refers to the number and complexity of connections between 'calling' and 'called' modules.

In a good modular design, cohesion should be high and coupling should be low.

22. (a) The IS control Audit process involves the following:

- Obtaining an understanding of an entity and its operations and key business processes,
- Obtaining a general understanding of the structure of the entity's networks,
- Identifying key areas of audit interest (files, applications, systems, locations),
- Assessing IS risk on a preliminary basis,
- Identifying critical control points (for example, external access points to networks),
- Obtaining a preliminary understanding of IS controls, and
- Performing other audit planning procedures.

(b) Intrusion detection is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise the system and network resources of an organization. Intrusion Detection systems fall into two broad categories, which are given as follows:

- Network based systems: These types of systems are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries.
- Host based systems: These types of systems actually run on the system being monitored. These examine the system to determine whether the activity on the system is acceptable.

A more recent type of intrusion detection systems are those that reside in the operating system kernel and monitor activity at the lowest level of the system. These systems have recently started becoming available for a few platforms, and are relatively platform specific.

(c) Auditors' role in the change management process is given as follows:

- To evaluate the quality of decisions made with respect to project management and change facilitation;
- If the proposed system is small, it has a localized impact on users and change management can be done in-house with less material concerns; and

- If the proposed system is large, it has high-levels of requirements and technological uncertainty and organization structures and jobs will have significant effect.

23. (a) **Vulnerability:** It is the weakness in the system safeguards that exposes the system to threats. It may be weakness in an information system, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. Here, two more vulnerability examples are given as under:

- Leaving your front door unlocked makes your house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make your automated information system vulnerable to password cracking or guessing routines.

Missing safeguards often determine the level of vulnerability. Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, testing, and penetration analysis.

Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

Attack: This is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system. Simply, it is the act of trying to defeat IS safeguards. The type of attack and its degree of success will determine the consequence of the attack.

(b) Two primary questions, which should be considered while evaluating the risk, inherent in a business function are given as follows:

- What is the probability that things can go wrong? (*Probability*) This view will have to be taken strictly on the technical point of view and should not be mixed up with past experience. While deciding on the class to be accorded, one has to focus on the available measures that can prevent such happenings.
- What is the cost if 'what can go wrong' does go wrong? (*Exposure*)

Risk is evaluated by answering the above questions for various risk factors and assessing the probability of failure and the impact of exposure for each risk factor. Risk is the probability times the exposure.

© The Institute of Chartered Accountants of India

(c) [Section 3] Authentication of Electronic Records of ITAA 2008:

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

24. (a) There are a number of fact-finding techniques, which are used by the system analysts for determining the needs/requirements of different modules namely, documents, questionnaires, interviews, and observations. Some brief discussion on first two techniques is briefly discussed below:

- Documents: Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc. Documents are a very good source of information about user needs and the current system.
- Questionnaires: Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.

© The Institute of Chartered Accountants of India

(b) The goals of a business continuity plan are stated below:

- 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.

(c) Major backup tips are given as follows:

- Draw up a simple (easy to understand) plan of who will do what in the case of an emergency.
- Be organized and Keep a record of 'what was backed up', 'when it was backed up' and 'which backup media contains what data'. We can also make a calendar of 'which type of backup is due on a certain date'.
- Select the option to verify backup; the process will take a little longer but it's definitely worth the wait.
- Create a reference point where we know everything is working properly. It will be quicker to restore the changes from tape.
- Select the option to restrict restoring data to owner or administrator and also set the Domain Group Policy to restrict the Restore privilege to Administrators only. This will help to reduce the risk of someone being able to restore data should the media be stolen.
- Create a step-by-step guideline (a flowchart for example) clearly outlining the sequence for the retrieval and restoration of data depending on the state of the system.

25. (a) Some popular expectations from an ERP solution are stated below:

- An improvement in processes;
- Increased productivity on all fronts;
- Total automation and disbanding of all manual processes;
- Improvement of all key performance indicators;
- Elimination of all manual record keeping;
- Real time information systems available to concerned people on a need basis; and
- Total integration of all operations.

(b) The Change Control process of a system under development is to address the problems not detected during system design or testing and change in user requirements. A change control evaluation includes checks on problems reporting, tracking, prioritizing, and resolving, and if changes are authorized, tested, documented, and communicated through a legitimate management responsibility. The risks dealt with the change control processes are given as under:

- System outages due to error, omissions, or malicious intent,
- Data loss or errors due to error, omissions, or malicious intent,
- Unauthorized changes,
- Fraud/abuse to company systems and/or data,
- Repeated errors, and
- Reruns of system or application processes.

The objective of a change management review is to ensure that changes made to the system and programs do not adversely affect system, application, or data availability or integrity. Auditors need to verify that all changes made to the systems and programs are appropriately authorized and documented.

(c) The controls and objectives of System Development and Maintenance are enumerated below:

- *Security requirements of system*: To ensure that security is built into information systems;
- *Security in application systems*: To prevent loss, modification or misuse of user data in application system;
- *Cryptographic Controls*: To protect the confidentiality, authenticity or integrity of information;
- *Security of system files*: To ensure that IT projects and support activities are conducted in a secure manner; and
- *Security in development and support process*: To maintain the security of application system software and information.

© The Institute of Chartered Accountants of India