PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Information Systems Concepts

1. (a) Discuss major characteristics of an effective MIS.

   (b) 'There is a practical set of principles, which is used to guide the design of measures and indicators to be included in an EIS'. Explain these principles in brief.

2. What do you mean by an Expert System? Explain some of its business applications.

Software Development Life Cycle Methodology

3. What is Waterfall Model? Describe its strengths and weaknesses in brief.

4. (a) Discuss basic principles of Prototyping Model in brief.

   (b) What are the major activities that are performed in the requirements analysis phase of the SDLC?

5. (a) What is Integration testing? Explain bottom-up and top-down integration.

   (b) Discuss System testing along with its other associated testing techniques.

Control Objectives

6. (a) What do you mean by Detective Controls? Explain with the help of examples.

   (b) Explain major Boundary Control Techniques in brief.

7. 'There are a number of general questions that an auditor will need to consider for quality control'. Explain those questions in brief.

8. (a) Briefly describe various activities involved in a conversion process during system implementation. Also explain different strategies used in a conversion process.

   (b) Discuss Packet Filter Firewalls along with their major weaknesses.

Testing – General and Automated Controls

9. (a) Discuss major disadvantages/limitations of the Continuous Audit System in brief.

   (b) Explain the term 'testing' with reference to controls. Also define substantive and compliance testing.

Risk Assessment Methodologies and Applications

10. (a) Briefly explain the following terms:

    (i) Threat,

    (ii) Vulnerability,

    (iii) Exposure,

© The Institute of Chartered Accountants of India

(iv) Likelihood, and

(v) Attack.

(b) Describe common risk mitigation techniques.

Business Continuity Planning and Disaster Recovery Planning

11. (a) Briefly explain the goals of a business continuity plan.

(b) Describe some of the important backup tips, which must be kept in mind while taking the backup.

An Overview of Enterprise Resource Planning (ERP)

12. 'Organizations face several new business risks when they migrate to real-time, integrated ERP systems'. What are those risks?

Information Systems Auditing Standards, Guidelines, Best Practices

13. Define the following terms:

(i) Software Process Capability,

(ii) Software Process Performance, and

(iii) Software Process Maturity

14. Discuss controls and objectives of 'Communications and Operations Management'.

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

15. (a) Discuss the important points, which need to be taken into consideration for asset and security classification.

(b) Briefly explain the contents of a permanent audit file.

Information Technology (Amendment) Act 2008

16. (a) Discuss the Electronic Signature under Section 3A of Information Technology (Amendment) Act, 2008.

(b) Describe the Duties of Certifying Authorities in the light of Section 30 of Information Technology (Amendment) Act, 2008.

17. Discuss the 'Power to authorize and collect traffic data or information through any computer resource for Cyber Security' under Section 69B of Information Technology (Amendment) Act, 2008.

Questions based on Short Notes

18. Write short notes on the following:

(a) Technical Feasibility

© The Institute of Chartered Accountants of India

(b) Final Acceptance Testing

(c) Delphi Technique for risk evaluation

19. Write short notes on the following:

(a) Cold Site and Hot Site

(b) Spoofing

(c) Constraints in operating a MIS

20. Write short notes on the following:

(a) Program Debugging

(b) Big Bang and Phased Implementation of ERP

(c) Recognition of Foreign Certifying Authorities in the light of Section 19 of Information Technology (Amendment) Act, 2008

Questions based on the Case Studies

21. ABC India Ltd. is a leading company dealing in the retail market. Store operations have never been as important to retailers as they are now. Successful retailers are those, who know that the battle for customers is only won at the frontline, which in the case of a retail chain is at its stores. The company was regularly opening stores in the metros and there was an urgent need for a reliable enterprise wide application to help and run its business effectively. The basic need was to have a robust transaction management system and an enterprise wide platform to run the operations. The company was looking for a solution that would bring all of its businesses and processes together. After a comprehensive evaluation of different options, the management of the company decided to go for an ERP solution to keep itself competitive in the rapidly growing Indian retail market.

Read the above carefully and answer the following:

(a) What do you mean by ERP Systems? Explain in brief.

(b) Do you agree or disagree with the decision of the management? Validate your answer in any of the case with suitable points.

(c) 'ERP implementation also engenders a host of fears'. Briefly explain those fears.

22. PQR Ltd. is a petrochemical company, which produces various chemicals that are shipped to clients worldwide. It receives raw materials, supplies, feedstock (Ethane, Benzene, Methanol, etc.) and utilities (cooling water, gas, electricity, etc.) from private and public organizations within and outside the industrial city. The petrochemical complex consists of six production units (each producing a specific chemical product); offices within the main plant for engineers and operations personnel; offices outside the main plant area housing the head office functions (finance, HR, etc.); various other buildings (warehouses, security stations, etc.); and, IT and telecoms centers. After a

© The Institute of Chartered Accountants of India

detailed initial analysis and extensive stakeholders' engagement, the company decided to introduce Business Continuity Planning (BCP) for each Production Unit (PU) head offices (including computer / telecoms centre and security) and for the operations offices (located within the plant). For each PU BCP, a technical BCP development team was formed consisting of production engineers, technical specialists, production control and automation experts, process safety engineers and an external technical BCP facilitator. Each team was led by the PU manager. For the office BCP, the BCP development team consisted (as is usually the case) of representatives from the main functions (finance, etc.), IT, telecoms and an external office BCP facilitator. The team was led by the finance director. The business continuity plan development methodology applied was based on the appropriate standard, as the company wanted to lead the way in the region in the adoption of the standard.

Read the above carefully and answer the following:

(a) What is BCP? Explain the major areas covered by it.

(b) 'Generally, the methodology for developing a business continuity plan may be sub-divided into eight different phases. However, the extent of applicability of each of the phases has to be tailored to the respective organization'. Briefly describe major points emphasized by the methodology.

(c) In what way, the company decided to introduce BCP for its different units and offices.

23. At one point of time, software development consisted of a programmer, writing code to solve a problem or automate a procedure. Nowadays, systems are so big and complex that teams of architects, analysts, programmers, test engineers and users must work together to create the millions of lines of custom-written code that drive our enterprises. To manage all these activities, Software Development Life Cycle (SDLC) came into the picture. SDLC is a formalized, standardized, documented set of activities used to manage system development projects. It refers to a framework that is used to structure, plan and control the process of developing an information system. To accomplish various tasks, a number of SDLC models have been innovated namely, waterfall, spiral, rapid prototyping, incremental, and agile etc. Each of the available models is a 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) Discuss the strengths of Rapid Application Development (RAD).

(b) 'Feasibility Study plays an immense role in SDLC'. What are the various dimensions, under which feasibility study of a system is carried out?

(c) How accountants can be involved in the development work? Give your opinion.

© The Institute of Chartered Accountants of India

24. PQR Ltd. is one of the best-known computer software companies. The company's vision, shaped by its founders was to empower people through a good quality software. The company offered a wide range of software products for various computing devices. These included scalable operating systems for servers, personal computers (PCs), and intelligent devices; server applications for client/server environments; information worker productivity applications; business solutions/applications and software development tools. The company covers four major business areas for software development: Desktop and Enterprise Software and Services; Consumer Software, Services, and Devices and Consumer Commerce Investments. As we know that information security is of prime concern for everyone in today's vulnerable environment, the company has also embarked on a long-term initiative, which aimed at providing an enhanced level of security, privacy, reliability, and business integrity to computer systems.

    Read the above carefully and answer the following:

    (a) How the company is achieving its vision to empower people through good quality software?

    (b) 'Confidentiality', 'Integrity', and 'Availability' are three globally accepted attributes of Information Security. Briefly explain these terms and their main objectives.

    (c) What should be the major components of a good information security policy as per your opinion?

25. XYZ Ltd. is a leading company in the manufacturing of biscuits. The company is in the process of automation of its various business processes. During this automation, technical consultant of the company highlighted the importance of information security and suggested to introduce it *right from the beginning*. He also suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risks. For implementation of all these suggestions, various best practices have been followed by the company. In addition, after each activity, appropriate standards' compliances have also been tested to check the quality of each process. Various policies related with business continuity planning and disaster recovery planning have been implemented to ensure three major expectations from the software: resist, tolerate and recover.

    Read the above carefully and answer the following:

    (a) What are the major suggestions given by the technical consultant? How the company is implementing those suggestions?

    (b) Discuss risk assessment with the help of risk analysis framework in brief.

    (c) 'Different types of plans are used in BCP namely, Emergency Plan, Back-up Plan, Recovery Plan, and Test Plan'. Discuss recovery plan in brief.

© The Institute of Chartered Accountants of India

SUGGESTED ANSWERS/HINTS

1. (a) Major characteristics of an effective MIS are briefly discussed below:

(i) Management Oriented: It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessary for top management only, it may also meet the information requirements of middle level or operating levels of management as well.

(ii) Management Directed: Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but also for its review as well to ensure that the implemented system meets the specifications of the designed system.

(iii) Integrated: Development of information should be integrated, which means that all the functional and operational information sub-systems should be tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management by taking a comprehensive view or a complete look at inter locking sub-systems that operate within a company.

(iv) Common Data Flows: It provides a facility for the use of common input, processing and output procedures and media whenever required. Data is captured by system analysts only once and as close to its original source as possible. Afterwards, they, try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.

(v) Heavy Planning Element: An MIS usually takes three to five years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development who should keep in view future objectives and requirements of firm's information in mind.

(vi) Sub System Concept: Even though the information system is viewed as a single entity, it must be broken down into logical sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.

(vii) Common Database: Database is the mortar that holds the functional systems together. It is defined as a "super-file" which consolidates and integrates data

© The Institute of Chartered Accountants of India

records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.

(viii) Computerized: Though MIS can be implemented without using a computer, the use of computers increases the effectiveness of the system. In fact, its usage equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

(b) A practical set of principles to guide the design of measures and indicators to be included in an EIS is presented below:

(i) EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.

(ii) 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.

(iii) 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.

(iv) 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.

(v) 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.

(vi) EIS measures must evolve to meet the changing needs of the organization.

2. An Expert System is highly developed DSS that utilizes knowledge, generally possessed by an expert to share a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – 'how much can be

© The Institute of Chartered Accountants of India

invested? Does the client have any preferences regarding specific types of securities?' And other similar questions.

Some of the business applications of Expert Systems are as follows:

(i) Accounting and Finance: It provides tax advice and assistance, helping with credit-authorization decisions, selecting forecasting models, Providing investment advice.

(ii) Marketing: It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centres, assisting with marketing timing decisions, determining discount policies.

(iii) Manufacturing: It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.

(iv) Personnel: It is useful in assessing applicant qualifications, giving employees assisting at filling out forms

(v) General Business: It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

3. Waterfall approach is a traditional development approach in which each developer in a development team works in different phases. These phases include requirement analysis, specifications and design, coding, final testing, and release. The waterfall approach is used on small projects because it eliminates testing to identity problems early in the process.

Strengths

(i) This approach is an Ideal approach for supporting less experienced project teams and project managers or project teams whose composition fluctuates.

(ii) An orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.

(iii) Progress of system development is measurable, in case waterfall Model is followed.

(iv) This approach is also helpful in conserving resources.

Weaknesses

(i) Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.

(ii) Project progresses forward, with only slight movement backward.

(iii) Little room for use of iteration, which can reduce manageability if used.

(iv) It depends upon early identification and specification of requirements, yet users may not be able to clearly define what they need early in the project.

© The Institute of Chartered Accountants of India

(v) Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.

(vi) Problems are often not discovered until system testing.

(vii) System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.

(viii) Difficult to respond to changes. Changes that occur later in the life cycle are more costly and are thus discouraged.

(ix) Produces excessive documentation and keeping it updated as the project progresses is time-consuming.

(x) Written specifications ate often difficult for users to read and thoroughly appreciate.

(xi) Promotes the gap between users and developers with clear vision of responsibility.

4. (a) Basic Principles of Prototyping Model : Prototyping can be viewed as a series of four steps, depicted in the Fig., wherein Implementation and Maintenance phases take place once the prototype model is tested and found to be meet uses' requirements. These steps are given as follows:

Step 1 - Identify Information System Requirements: In traditional approach, the system requirements have to be identified before the development process starts. However, under prototype approach, the design team needs only fundamental system requirements to build the initial prototype, the process of determining them can be less formal and time-consuming than when performing traditional systems analysis.

Step 2 - Develop the Initial Prototype: In this step, the designers create an initial base model and give little or no consideration to internal controls, but instead emphasize such system characteristics such as simplicity, flexibility, and ease of use. These characteristics enable users to interact with tentative versions of data entry display screens, menus, input prompts, and source documents. The users also need to be able to respond to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.

Step 3 - Test and Revise: After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment and ask users to record their likes and dislikes about the system and recommend changes. Using this feedback, the design team modifies the prototype as necessary and then resubmits the revised model to system users for revaluations. Thus iterative process of modification and revaluation continues until the users are satisfied.

Step 4 - Obtain User Signoff of the Approved Prototype: At the end of Step 3, users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not, do or provide.

© The Institute of Chartered Accountants of India

Prototyping is not commonly used for developing traditional applications such as accounts receivable, accounts payable, payroll, or inventory management, where the inputs, processing, and outputs are well known and clearly defined.

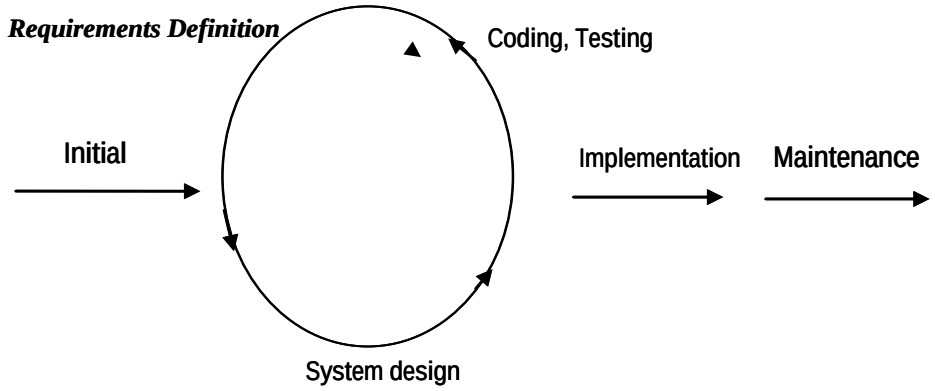

Fig. : Prototyping Model

(b) Requirements Analysis phase of the SDLC includes a thorough and detailed understanding of the current system, identification of the areas that need modification to solve the problem, the determination of user/managerial requirements and to have fair idea about various systems development tools.

The following are the major activities, which are performed in this phase:

- To identify and consult the stake owners to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine priorities;
- To verify the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like - interviewing, research/document collection, questionnaires, observation;
- To model activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modelling activities.

5. (a) Integration Testing : This is an activity of software testing in which individual software modules are combined and tested as a group. It occurs after unit testing

© The Institute of Chartered Accountants of India

and before system testing with an objective to evaluate the connection of two or more components that pass information from one area to another. Integration testing takes as its input - modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing. This is carried out in the following manner:

- Bottom-up Integration: This is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub-system testing, and then testing of the entire system. Bottom-up testing is easy to implement as at the time of module testing, tested subordinate modules are available. Main disadvantage is that testing of major decision / control points is deferred to a later period.
- Top-down Integration: This starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module. An incomplete portion of a program code that is put under a function in order to allow the function and the program to be compiled and tested, is referred to as a stub. A stub does not go in to the details of implementing details of the function or the program being executed.

Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested with stubs. This process continues till the atomic modules are reached. Since decision- making processes are likely to occur in the higher levels of program hierarchy, the top-down strategy emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes. The difficulty arises in the top-down method, because the high-level modules are tested, not with real outputs from subordinate modules, but from stubs.

(b) System Testing: System testing is a process in which software and other system elements are tested as a whole. System testing begins either when the software as a whole is operational or when the well defined subsets of the software's functionality have been implemented. The purpose of system testing is to ensure that the new or modified system functions properly. These test procedures are often performed in a non- production test environment. The types of testing that might be carried out are as follows:

- Recovery Testing: This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is properly performed.
- Security Testing: This is the process to determine that an Information System protects data and maintains functionality as intended or not. The six basic security concepts that need to be covered by security testing are –

© The Institute of Chartered Accountants of India

confidentiality, integrity, authentication, authorization, availability and non-repudiation. This testing technique also ensures the existence and proper execution of access controls in the new system.

- Stress or Volume Testing: Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.
- Performance Testing: In the computer industry, software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

6. (a) Detective Control: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. Examples of detective controls include:

- Hash totals,
- Check points in production jobs,
- Echo control in telecommunications,
- Error message over tape labels,
- Duplicate checking of calculations,
- Periodic performance reporting with variances,
- Past-due accounts report,
- The internal audit functions,
- Intrusion detection system,
- Cash counts and bank reconciliation, and
- Monitoring expenditures against budgeted amount

(b) Major boundary control techniques are given as follows:

- *Cryptography:* It deals with programs for transforming data into codes that are meaningless to anyone who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution)

© The Institute of Chartered Accountants of India

- *Passwords*: User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.
- *Personal Identification Numbers (PIN):* The personal identification number is similar to a password assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm, or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number. Hence a PIN or a digital signature are exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- *Identification Cards*: Identification cards are used to store information required in an authentication process. These cards used to identify a user are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.

7. The following are the general questions that the auditor will need to consider for quality control:
   - Does the system design follow a defined and acceptable standard?
   - Are completed designs discussed and agreed with the users?
   - Does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organization's technical standards and policies, and the User Requirements Specification;
   - Do quality reviews follow a defined and acceptable standard?
   - Are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;
   - Are auditors/security staffs invited to comment on the internal control aspects of system designs and development specifications?
   - Are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
   - Are defects uncovered during quality reviews always corrected?
   - Are all system resources (hardware, software, documentation) that have passed quality review been placed under change control management and version control?

© The Institute of Chartered Accountants of India

- Has a System Installation Plan been developed and quality reviewed?
- Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery? (to avoid "skills stagnation", the delivery of training will need to be carefully scheduled)?

8. (a) Conversion process during system implementation involves the following major activities:

- Defining the procedures for correcting and converting data into the new application, determining what data can be converted through software and what data manually.
- Performing data cleansing before data conversion,
- Identifying the methods to access the accuracy of conversion like record counts and control totals,
- Designing exception reports showing the data which could not be converted through software, and
- Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

Major conversion strategies are given as follows:

- *Direct implementation / Abrupt change-over*: In such strategies, the old system is suspended on a specific day and the new system is implemented. It reduces cost of redundant processing but in case of a failure due to say a system crashes, the old system is also not available for recovery. In case of small applications, or when migrating from a manual to computer system, this may be used.
- *Parallel implementation*: Both the old and new systems are run in parallel to verify if their output is the same. Then the old system is suspended. Here redundant processing is costly but reduces risks associated with conversion. But users will face problems in working with both systems.
- *Phased implementation*: This strategy consists of implementing the new system in parts. This makes implementation more manageable. This is also called the phase-in conversion and provides a steady transition.
- *Pilot implementation*: The new systems is first implemented in modules of non-critical units and then moved to larger unit.

Except direct implementation, others strategies are not mutually exclusive. A cautious combination of the strategies can be adopted, depending on the type of application/ system.

© The Institute of Chartered Accountants of India

(b) Packet Filter Firewalls: Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filters generally do not analyze the packet contents beyond the header information. Many routers contain access control lists (ACLs) that allow for packet-filtering capabilities.

Dynamic packet filtering incorporates an inspection primarily for performance benefits. Before re-examining every packet, the firewall checks each packet as it arrives to determine whether it is part of an existing connection. If it verifies that the packet belongs to an established connection, then it forwards the packet without subjecting it to the firewall rule set.

Weaknesses associated with packet filtering firewalls include the following:

- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.
- Logging functionality is limited to the same information used to make access control decisions.
- Most of them do not support advanced user authentication schemes.
- Firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
- The firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.

9. (a) The following are major disadvantage/limitations of the use of the continuous audit system:

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

© The Institute of Chartered Accountants of India

(b) Testing is a scientific process performed to determine whether the controls ensure the system design effectiveness as well as the implemented system controls operational effectiveness. It involves, understanding a process and the expected results. Testing of large amounts of transactions or data is usually not possible due to time and cost constraints. Hence, sampling is done on the population (system resource) and ensures a sufficient quality and quantity to extrapolate the results of the testing into a reliable conclusion on the entire population (system resource).

Testing of Controls involves obtaining the population and conducting the compliance tests either on the entire population and/or on selected samples from the population. It may also be conducted using utilities of audit tools. Testing of the controls design and the reliable results are done by one of the following methods:

- *Substantive Testing:* This type of testing is used to substantiate the integrity of the actual processing. It is used to ensure that processes, not controls, are working as per the design of the control and produce the reliable results.
- *Compliance Testing* – A compliance test determines if controls are working as designed. As per the policies and procedures, compliance testing results into the adherence to management directives.

10. (a) (i) Threat: A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organisation. Threat is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services.

(ii) Vulnerability: This 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.

(iii) Exposure: An exposure is the extent of loss the organisation has to face when a risk materialises. It is not just the immediate impact, but the real harm that occurs in the long run. For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources.

(iv) 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.

(v) Attack: This is a set of actions designed to compromise confidentiality,

© The Institute of Chartered Accountants of India

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) Mitigation and measurement techniques are applied according to the event's losses, and are measured and classified according to the loss type. Some of the common risk mitigation techniques are given as follows:

- Insurance**:** An organization may buy insurance policies to mitigate such risk. Under the scheme of the insurance, the loss is transferred from the insured entity to the insurance company in exchange of a premium. However while selecting such an insurance policy one has to look into the exclusion clause to assess the effective coverage of the policy. Under the Advanced Management Approach under Basel II norms (AMA), a bank will be allowed to recognize the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements. The recognition of insurance mitigation is limited to 20% of the total operational risk capital charge calculated under the AMA.

- Outsourcing**:** The organization may transfer some of the functions to an outside agency and transfer some of the associated risks to the agency. One must make careful assessment of whether such outsourcing is transferring the risk or is merely transferring the management process. For example, outsourcing of telecommunication line viz. subscribing to a leased line does not transfer the risk. The organization remains liable for failure to provide service because of a failed telecommunication line. Consider the same example where the organization has outsourced supply and maintenance of a dedicated leased line communication channel with an agreement that states the minimum service level performance and a compensation clause in the event failure to provide the minimum service level results in to a loss. In this case, the organization has successfully mitigated the risk.

- Service Level Agreements**:** Some of risks can be mitigated by designing the service level agreement. This may be entered into with the external suppliers as well as with the customers and users. The service agreement with the customers and users may clearly exclude or limit responsibility of the organization for any loss suffered by the customer and user consequent to the technological failure. Thus a bank may state that services at ATM are subject to availability of service there and customers need to recognize that such availability cannot be presumed before claiming the service. The delivery of service is conditional upon the system functionality. Whereas the service is guaranteed if the customer visits the bank premises within the banking hours.

© The Institute of Chartered Accountants of India

It must be recognized that the organization should not be so obsessed with mitigating the risk that it seeks to reduce the systematic risk - the risk of being in business. Cost-benefit analysis must be done for adapting the risk mitigation tools.

11. (a) The goals of a business continuity plan should be to:

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

(b) Some of the important 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! Keep a record of what was backed up, when it was backed up and which backup media contains what data. You can also make a calendar of which type of backup is due on a certain date.
- Utilize the Volume Shadow Copy (VSS) service in Windows Server 2003. This feature allows you to create point-in-time copies of data so that they can be restored and reverted to at any given time. For instance, if a user created a Word document yesterday and decides that he wants to revert to it today, he can do so using VSS.
- 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 you 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.

12. Major business risks faced by the organizations while migrating to real-time, integrated ERP systems, are given as follows:

- *Single point of failure:* Since all the organization's data and transaction processing is within one application system and transaction processing is within one application system.
- *Structural changes:* Significant personnel and organizational structures changes associates with reengineering or redesigning business processes.

© The Institute of Chartered Accountants of India

- *Job role changes:* Transition of traditional user's roles to empowered-based roles with much greater access to enterprise information in real time and the point of control shifting from the back-end financial processes to the front-end point of creation.
- *Online, real-time*: An online, real-time system environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring of re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).
- *Change management*: It is challenging to embrace a tightly integrated environment when different business processes have existed among business units for so long. The level of user acceptance of the system has a significant influence on its success. Users must understand that their actions or inaction have a direct impact upon other users and, therefore, must learn to be more diligent and efficient in the performance of their day-to-day duties. Considerable training is therefore required for what is typically a large number of users.
- *Distributed computing experience*: Inexperience with implementing and managing distributed computing technology may pose significant challenges.
- *Broad system access*: Increased remote access by users and outsiders and high integration among application functions allow increased access to application and data.
- *Dependency on external assistance*: Organization accustomed to in-house legacy systems may find they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to greater risk.
- *Program interfaces and data conversions:* Extensive interfaces and data conversions from legacy systems and other commercial software are often necessary. The exposures of data integrity, security and capacity requirements for ERP are therefore often much higher.
- *Audit expertise:* Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know only a relatively small fraction of the entire ERP's functionality in a particular core module, e.g. FI auditors, who are required to audit the entire organization's business processes, have to maintain a good grasp of all the core modules to function effectively.

13. (i) Software Process Capability: It describes the range of expected results that can be achieved by following a software process. The software process capability of an

© The Institute of Chartered Accountants of India

organization provides one means of predicting the most likely outcomes to be expected from the next software project the organization undertakes.

(ii) Software Process Performance: It represents the actual results achieved by following a software process. Thus, software process performance focuses on the results achieved, while software process capability focuses on results expected.

(iii) Software Process Maturity: This is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods, practices, and procedures of the business so that they endure after those who originally defined them have gone.

14. The control and objectives of 'Communications and Operations Management' are given as follows:

- *Operational procedures and responsibilities:* To ensure correct and secure operation of information processing facility;
- *System planning and acceptance :* To minimize risks of system failure;
- *Protection against malicious software:* To protect the integrity of software and information;
- *Housekeeping:* To maintain the integrity and availability of information processing and communication services;
- *Network Management*: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
- *Media handling and security:* Prevent damage to assets and interruptions to business activity; and
- *Exchanges of information and software:* To prevent loss, modification or misuse of information exchanged between organizations.

15. (a) Following are the major points, which are needed to be taken into consideration for asset and security classifications:

- An inventory of assets must be maintained. This must include physical, software and information assets.
- A formal, documented classification scheme (as set out in the Information Classification Policy) should be in place and all staff must comply with it.

© The Institute of Chartered Accountants of India

- The originator or 'owner' of an item of information (e.g. a document, file, diskette, printed report, screen display, e-mail, etc.) should provide a security classification, where appropriate.
- The handling of information, which is protectively marked CONFIDENTIAL or above must be specifically approved (i.e. above RESTRICTED).
- Exchanges of data and software between organizations must be controlled. Organizations to whom information is to be sent must be informed of the protective marking associated with that information, in order to establish that it will be handled by personnel with a suitable clearance corresponding to the protective marking.
- Appropriate procedures for information labeling and handling must be agreed and put into practice.
- Classified waste must be disposed of appropriately and securely.

(b) A permanent audit file normally includes the following:

- The organization structure of the entity,
- The IS policies of the organization,
- The historical background of the information system in the organization,
- Extracts of copies of important legal documents relevant to audit,
- A record of the study and evaluation of the internal controls related to the information system,
- Copies of audit reports and observations of earlier years, and
- Copies of management letters issued by the auditor, if any.

16. (a) [Section 3A] Electronic Signature :

(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub- section (2) a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which-

(a) is considered reliable ; and

(b) may be specified in the Second Schedule

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or , as the case may be, the authenticator and of no other person;

(b) the signature creation data or the authentication data were, at the time of

© The Institute of Chartered Accountants of India

signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfills such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.

(b) [Section 30] Duties of Certifying Authorities:

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

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

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

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

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

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

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

17. [Section 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security:

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the

© The Institute of Chartered Accountants of India

country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

18. (a) Technical Feasibility : It is concerned with the issues pertaining to hardware and software. Essentially, an analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following:

- Does the necessary technology exist to do what is suggested (and can it be acquired)?
- Does the proposed equipment have the technical capacity to hold the data required to use the new system?
- Can the proposed application be implemented with existing technology?
- Will the proposed system provide adequate responses to inquires, regardless of the number or location of users?
- Can the system be expanded if developed?
- Are there technical guarantees of accuracy, reliability, ease of access, and data security?

(b) Final Acceptance Testing: Final Acceptance Testing is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system satisfies the users. Thus, the final acceptance testing has two major parts:

- Quality Assurance Testing: It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance methodology.
- User Acceptance Testing: It ensures that the functional aspects expected by the users have been well addressed in the new system. There are two types of

© The Institute of Chartered Accountants of India

the user acceptance testing :

- Alpha Testing: This is the first stage, often performed by the users within the organization.
- Beta Testing: This is the second stage, generally performed by the external users. This is the last stage of testing, and normally involves sending the product outside the development environment for real world exposure.

(c) Delphi Technique for Risk Evaluation: The Delphi Technique was first used by the Rand Corporation for obtaining a consensus opinion. Here a panel of experts is appointed. Each expert gives his opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

19. (a) Cold Site: If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system-raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.

Hot Site: If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.

(b) Spoofing: A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that he is interacting with the operating system. For example, a penetrator duplicates the logon procedure, captures the user's password, attempts for a system crash and makes the user login again. It is only the second time the user actually logs into the system.

(c) Constraints in operating a MIS: Major constraints, which come in the way of operating an information system, given as follows:

- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing and operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.

© The Institute of Chartered Accountants of India

- Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts, depend upon the need and importance of a function for which MIS can be installed first.
- Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.
- Non-availability of cooperation from staff is a crucial problem which should be handled tactfully. This task should be carried out by organizing lecturers, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

20. (a) Program Debugging : Debugging is the most primitive form of testing activity which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by the programmer into machine language instructions. Debugging can be a tedious task consisting of following four steps:

- Inputting the source program to the compiler,
- Letting the compiler find errors in the program,
- Correcting lines of code that are erroneous, and
- Resubmitting the corrected source program as input to the compiler.

(b) "Big Bang" and Phased Implementation of ERP

A "big bang" implementation of ERP involves 'having all modules at all locations implemented at the same time'. Characteristics of this approach include:

- no need for temporary interfaces,
- limited requirement to maintain legacy software,
- cross-module functionality and
- overall cost if no contingencies arise.

Phased implementation of ERP means implementation of one or a group at a time, often a single location at a time. Benefits of this approach include:

- a smoothing of resource requirements,
- an ability to focus on a particular module,
- avail-ability of existing legacy systems as a fall-back,
- reduced risk,

© The Institute of Chartered Accountants of India

- the knowledge gained with each phase and
- the usefulness of demonstrable working system.

(c) Section 19 provides the powers to the Controller with the previous approval of the Central Government to grant recognition to foreign Certifying Authorities subject to such conditions and restrictions as may be imposed by regulations. As per ITAA 2008, Section 19 is given as under:

[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.

21. (a) Enterprise Resource Planning (ERP) Systems : ERP is one of the latest high-end solutions that seek to streamline and integrate operation processes and information flows in the company to synergize the five major resources of an organization namely men, money, machine, materials and market. Formally, ERP can be defined as follows:

"An ERP system is a fully integrated business management system that integrates the core business and management processes to provide an organization a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable real-time information."

(b) Yes, we agree with the decision of the management. Major points for supporting their decision are given as follows:

- It provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.
- It supports strategic and business planning activities, operational planning and execution activities etc. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.
- It facilitates company-wide Integrated Information System covering all functional areas like manufacturing, selling and distribution, payables,

© The Institute of Chartered Accountants of India

receivables, inventory, accounts, human resources, purchases etc.

- It provides complete integration of systems not only across departments but also across companies under the same management.
- It is the solution for better project management.
- It allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Internet, Intranet, Video conferencing, E-Commerce etc.
- It eliminates most business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
- It provides intelligent business tools like decision support system, Executive information system, Data mining and easy working systems to enable better decisions.

(c) ERP implementation also engenders a host of fears. Some of these fears are given as under:

- Job redundancy;
- Loss of importance as information is no longer an individual prerogative;
- Change in job profile;
- An organizational fear of loss of proper control and authorization;
- Increased stress caused by greater transparency; and
- Individual fear of 'loss of authority'.

22. (a) Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for 'how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption'. The logistical plan is called a business continuity plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response.

Business continuity covers the following areas:

- *Business resumption planning:* The operation's piece of business continuity planning.
- *Disaster recovery planning:* The technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
- *Crisis management:* The overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

© The Institute of Chartered Accountants of India

(b) The methodology emphasizes on the following points:

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

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

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

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

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

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

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

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

(c) For the implementation of BCP, the company did a detailed analysis and decided to introduce BCP for its units and offices through different steps, which are given as follows:

- First of all, the company decided to introduce BCP for each Production Unit (PU
- Further, the company took over head offices, which include computer, telecoms centre and security.
- Afterwards, the company also included its operations offices, which are located within the plant.
- For each PU BCP, a technical BCP development team was formed consisting of production engineers, technical specialists, production control and automation experts, process safety engineers and an external technical BCP facilitator. Each team was led by the PU manager.
- For the office BCP, the BCP development team consisted (as is usually the case) from representatives from the main functions (finance, etc.), IT, telecoms and an external office BCP facilitator. The team was led by the Finance Director.
- For all the above mentioned activities related with the introduction of BCP, the company followed the appropriate standard to lead the way in the region.

© The Institute of Chartered Accountants of India

23. (a) Major strengths of RAD are given as follows:

- The operational version of an application is available much earlier than with Waterfall, Incremental, or Spiral frameworks, if RAD is adapted.
- Since RAD produces systems more quickly and to a business focus, this approach tends to produce systems at lower cost.
- Quick initial reviews are possible.
- Constant integration isolates problems and encourages customer feedback.
- RAD holds a great level of commitment from stakeholders, both business and technical, than Waterfall, Incremental, or spiral frameworks. Users are seen as gaining more of a sense of ownership of a system, while developer are seen as gaining more satisfaction from producing successful systems quickly.
- It concentrates on essential system elements from user viewpoint.
- It provides the ability to rapidly change system design as demanded by users.
- It produces a tighter fit between user requirements and system specifications.
- RAD generally produces a dramatic savings in time, money and human effort.

(b) The Feasibility Study of a system is evaluated under the following major dimensions:

- *Technica*l: Is the technology needed available?
- *Financia*l: 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?
- *Behavioural:* Is the solution going to bring any adverse effect on quality of work life?
- *Legal:* Is the solution valid in legal terms?

(c) Accountants' involvement in Development work: Many accountants are uniquely qualified to participate in systems development because they may be among the few people in an organization who can combine knowledge of IT, business, accounting, and internal control, as well as behaviour and communications. Through their abilities, they can ensure that new systems meet the needs of the user and possess adequate internal controls. Since, they have specialized skills such as accounting and auditing, they can apply their skills to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits.

© The Institute of Chartered Accountants of India

24. (a) The company is achieving its vision to empower people through good quality software by the following ways:

- By offering a wide range of software products for various computing devices; which include:
  - scalable operating systems for servers, personal computers (PCs), and intelligent devices,
  - server applications for client/server environments,
  - information worker productivity applications,
  - business solutions/applications and
  - software development tools.
- By embarking on a long-term initiative, which aimed at providing an enhanced level of:
  - security,
  - privacy,
  - reliability, and
  - business integrity to computer systems.

(b) Information Security comprises three universally accepted attributes, which are given as follows along with their main objectives:

- Confidentiality: It refers to the prevention of the unauthorized disclosure of information. The main objective of confidentiality is to ensure that only authorized user can have to the software/information access regardless of where the information is kept and how it is accessed. Confidentiality can be maintained by mechanism like access control, password, biometrics, encryption, privacy and ethics.
- Integrity: It refers to the prevention of the unauthorized modification of information. The main objective of integrity is to safeguard the accuracy and completeness of information and processing methods from being changed intentionally, unintentionally, or accidentally. Integrity is basically related with trustworthiness, which needs to be maintained for ensuring privacy, security and reliability of data and information. Integrity can be maintained by mechanisms like configuration management and auditing.
- Availability: It refers to the prevention of the unauthorized withholding of information. The main objective of availability is to ensure access of information and related assets for authorized users whenever needed. Availability can be maintained by mechanisms like data backup plan, disaster recovery plan, business continuity or resumption plan.

© The Institute of Chartered Accountants of India

(c) A good security policy should clearly state the following:

- Purpose and Scope of the Document and the intended audience,
- The Security Infrastructure,
- Security policy document maintenance and compliance requirements,
- Incident response mechanism and incident reporting,
- Security organization Structure,
- Inventory and Classification of assets,
- Description of technologies and computing structure,
- Physical and Environmental Security,
- Identity Management and access control,
- IT Operations management,
- IT Communications,
- System Development and Maintenance Controls,
- Business Continuity Planning,
- Legal Compliances,
- Monitoring and Auditing Requirements, and
- Underlying Technical Policy.

These are the major contents of a typical security policy. However, the policy is very organization specific and a study of the organizations' functions, their criticality and the nature of the information would determine the content of the security policy.

25. (a) During the automation of various processes of XYZ Ltd. the technical consultant of the company has given the following major suggestions:

- By realizing the importance of information security, he suggested to introduce it *right from the beginning*.
- In addition, he also suggested to perform the risk assessment activity.
- Finally, he advised to mitigate the assessed risks.

For the implementation of all the above mentioned suggestions, the company took the following steps:

- The company followed various best practices for each process for the proper implementation of the suggestions.
- In addition, the company also tested the compliance of appropriate standards' after each activity, to check the quality of each process.

© The Institute of Chartered Accountants of India

- Further, the company also implemented the policies related with business continuity planning and disaster recovery to ensure three broad expectations from the software: resist, tolerate and recover.

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

A risk analysis can provide an effective approach that will serve as the foundation for avoiding of disasters. Through risk analysis, it is possible to identify, assess, and then mitigate the risk. Such an analysis entails the development of a clear summary of the current situation and a systematic plan for risk identification, characterization, and mitigation. The framework of risk analysis is given as follows:

Fig.: Risk Analysis Framework

(c) Recovery Plan: The backup plan is intended to restore operations quickly so the information system function can continue to service an organisation, 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 organisation, new members must be appointed immediately and briefed about their responsibilities.

© The Institute of Chartered Accountants of India