

Questions Based on the Case Studies

Question 1

Worldwide, a global telecom company is serving to more than 10 million customers in the area of communications through fixed land lines, mobiles, internet services, digital TV and satellite system etc.

The financial analysts of the company are located in different functional groups in six geographical regions. These analysts are missing the access to the same data, as well as timely access to the information. Dated budget and actual numbers for each business unit reside in seven different systems, separating critical components of the Profit and Loss account and inhibiting analyst's ability to assess results. The problem gets further complicated as the field analysts are not able to go to one universal place to retrieve the data themselves and they have to rely upon the home office for the same.

The objective of the company is to set some critical financial goals so that the company could remain competitive and increase market share.

Read the above carefully and answer the following with justifications:

- (a) To overcome the problems which the financial analysts are facing, what kind of software the company should select?*
- (b) The company is advised that the adoption of BS7799 International Standard will help in overcoming the problems and achieving its goals. Discuss.*
- (c) How should the human resources be enriched for effective utilization of the proposed new systems and standards?*

Answer

- (a)** As the financial analysts of the company are working in six different geographical locations and the financial data is stored on seven different systems, located world wide, therefore they are facing several problems. Few of them are:

1. Missing the access to the same data as well as timely access to information.
2. Dated budget and actual numbers for each business unit reside in seven different systems, separating critical components of the profit and loss account thus failing the financial analysts to assess results.
3. The field analysts are not able to retrieve the data themselves from one universal place and therefore have to rely upon the home office for the same.

Therefore, the company should buy new software for the solution of the problems as mentioned above.

1.2 Information Systems Concepts

As far as software is concerned, of course the company should select the one which could make same data available to all the financial analysts. One such software is available from Oracle Corporation known as On Line Analytical Processing (OLAP) tool for better control over costs, analyze performance, evaluate opportunities, and formulate future directions. To improve the basis for making decisions, quickly and accurately with real time, consistent data which will improve cost control and to simplify and shorten the budgeting process, the software should be capable of:

1. Hands on ability to consolidate budgets, based on actual data in the process,
2. Enabling business units to make real-time, online decisions based on more accurate information,
3. User friendly.

The company is expected to be benefited by significant financial saving and therefore it should reduce the length of the budgeting cycle and the number of people involved in the process, thus keeping the company financially competitive in a growing market. The system should provide online, real time access to the information.

- (b) The BS 7799 (ISO 17799) consists of 127 best security practices which companies can adopt to build their Security Infrastructure. The model helps companies maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. The benefits of an ISMS tuned to the objective of the company are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact leading to increased profitability.

The company can use BS 7799 for the following reasons:

- .. Reduced operational risk,
- .. Increased business efficiency, and
- .. Assurance that information security is being rationally applied.

This is achieved by ensuring that:

- .. Security controls are justified.
- .. Policies and procedures are appropriate.
- .. Security awareness is good amongst staff and managers.
- .. All security relevant information processing and supporting activities are auditable and are being audited.
- .. Internal audit, incident reporting / management mechanisms are being treated appropriately.
- .. Management actively focus on information security and its effectiveness.

- (c) The human resources involved in the systems and standards can be enriched by the following activities:

Training Personnel: A system can succeed or fail depending on the way it is operated and used. Therefore, the quality of training received by the personnel involved with the system in various capacities helps in the successful implementation of information system and standards. Thus, training is a major component of systems implementation. When a new system is acquired which often involves new hardware and software, both users and computer experts need training organized by the vendor through hands-on learning techniques.

Training Systems Operators: The effective implementation of new systems and standards also depend on the computer-centre personnel, who are responsible for keeping the equipment running as well as for providing the necessary support services. Their training must ensure that they are able to handle all possible operations, both routine and extra-ordinary. As part of their training, operators should be given a trouble shooting list that identifies possible problems and remedies for them. Training also involves familiarization with run procedures, which involve working through the sequence of activities needed to use a new system on an on-going basis.

User training: User training deals with the operation of the system itself. Training in data coding emphasizes the methods to be followed in capturing data from transactions or preparing data for decision support activities. Users should be trained on data handling activities such as editing data, formulating inquiries (finding specific records or getting responses to questions) and deleting records of data. From time to time, users will have to prepare disks, load paper into printers, or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a micro computer or data entry system uses disks, users should be instructed in formatting and testing disks.

It is also required to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.

Question 2

ASK International proposes to launch a new subsidiary to provide e-consultancy services for organizations throughout the world, to assist them in system development, strategic planning and e-governance areas. The fundamental guidelines, programmes modules and draft agreements are all preserved and administered in the e-form only.

The company intends to utilize the services of a professional analyst to conduct a preliminary investigation and present a report on smooth implementation of the ideas of the new subsidiary. Based on the report submitted by the analyst, the company decides to proceed further with three specific objectives (i) reduce operational risk, (ii) increase business efficiency and (iii) ensure that information security is being rationally applied. The company has been advised to adopt BS 7799 for achieving the same.

1.4 Information Systems Concepts

- (a) *What are the two primary methods through which the analyst would have collected the data ?*
- (b) *To achieve their objectives, what are the points BS 7799 has to ensure ?*
- (c) *Suppose an audit policy is required, how will you lay down the responsibility of audit?*
- (d) *To retain their e-documents for specified period, what are the conditions laid down by Section 7, Chapter III of Information Technology (Amendment) Act, 2008?*

Answer

- (a) Two primary methods through which the analyst would have collected the data are given as follows:
 - (1) **Reviewing internal documents:** The analyst first tries to learn about the organization involved in or affected by the project. For example, to review an inventory system proposal, s/he will try to know 'how the inventory department operates' and 'who are the managers and supervisors'. S/he will examine organization charts and written operating procedures.
 - (2) **Conducting interviews:** Written documents tell the analyst 'how the system should operate' but they may not include enough details to allow a decision to be made about the merits of a system proposal nor do they present users' views about current operations. To learn these details, analysts use interviews. Preliminary investigation interviews involve only management and supervisory personnel.
- (b) **BS 7799 should ensure that:**
 - (1) Security controls are justified.
 - (2) Policies and procedures are appropriate.
 - (3) Security awareness is good amongst staff and managers.
 - (4) All security relevant information processing and supporting activities are auditable and are being audited.
 - (5) Internal audit, incident reporting/management mechanisms are being treated appropriately.
 - (6) Management actively focuses on information security and its effectiveness.
 - (7) Certification can also be used as a part of marketing initiative, providing assurance to business partners and other outsiders.
- (c) The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such

evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The audit policy should lay down the responsibilities as follows:

- (1) The policy should lay out the periodicity of reporting and the authority to whom the reporting is to be made.
 - (2) A statement of professional proficiency may be included to state the minimum qualification and experience requirements of the auditors.
 - (3) All information system auditors will sign a declaration of fidelity and secrecy before commencing the audit work in a form that the inspection department may design.
 - (4) The policy may lay out the extent of testing to be done under the various phases of the audit like Planning, Compliance Testing, and Substantive Testing.
 - (5) A documented audit program would be developed including the following:
 - “ Documentation of the information system auditor's procedures for collecting, analyzing, interpreting, and documenting information during the audit.
 - “ Objectives of the audit.
 - “ Scope, nature, and degree of testing required for achieving the audit objectives in each phase of the audit.
 - “ Identification of technical aspects, risks, processes, and transactions which should be examined.
 - “ Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.
 - (6) The policy should determine when and to whom the audit results would be reported and communicated. It would define the access rights to be given to the auditors.
 - (7) The Policy should outline the compliance testing areas.
 - (8) The auditor will carry out substantive testing wherever the auditor observes weakness in internal controls or where risk exposure is high. The auditor may also carry out such tests to gather additional information necessary to form an audit opinion.
 - (9) The Audit Policy would define the compulsory audit working papers to be maintained and their formats.
- (d)** Section 7, Chapter III of Information Technology (Amendment) Act, 2008 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:
- (i) The information therein remains accessible so as to be usable subsequently.

1.6 Information Systems Concepts

- (ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.
- (iii) The details which will facilitate the identification of the origin, destination, dates and time of dispatch or receipt of such electronic record are available therein.

This section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Moreover, this section does not apply to any law that provides for the retention of documents, records or information in the form of electronic records.

Question 3

ABC Industries Ltd., a company engaged in a business of manufacture and supply of automobile components to various automobile companies in India, had been developing and adopting office automation systems, at random and in isolated pockets of its departments.

The company has recently obtained three major supply contracts from International Automobile companies and the top management has felt that the time is appropriate for them to convert its existing information system into a new one and to integrate all its office activities. One of the main objectives of taking this exercise is to maintain continuity of business plans even while continuing the progress towards e-governance.

- (a) *When the existing information system is to be converted into a new system, what are the activities involved in the conversion process?*
- (b) *What are the types of operations into which the different office activities can be broadly grouped under office automation systems?*
- (c) *What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity.*
- (d) *What is the procedure to apply for a license to issue electronic signature certificates, under Section 22, Information Technology (Amendment) Act, 2008?*

Answer

- (a) Conversion from existing information system to a new system involves the following activities:
 - (i) Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually';
 - (ii) Performing data cleansing before data conversion;
 - (iii) Identifying the methods to assess the accuracy of conversion like record counts and control totals;
 - (iv) Designing exception reports showing the data which could not be converted through software; and

- (v) Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

(b) Types of Operations:

The types of operations into which different office activities under Office Automation Systems can be broadly grouped, are discussed as under:

- (i) **Document capture:** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.
- (ii) **Document Creation:** This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.
- (iii) **Receipts and Distribution:** This basically includes distribution of correspondence to designated recipients.
- (iv) **Filling, Search, Retrieval and Follow-up:** This is related to filling, indexing, searching of documents, which takes up significant time.
- (v) **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.
- (vi) **Recording Utilization of Resources:** This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

- (c) 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 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. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

- (i) **Business resumption planning** – The Operation's piece of business continuity planning;
- (ii) **Disaster recovery planning** – The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.
- (iii) **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.

1.8 Information Systems Concepts

- (d) Procedure to apply for a license to issue electronic signature under Section 22, IT (Amendment) Act, 2008 is given follows:
1. Every application for issue of a license shall be in such form as may be prescribed by the Central Government.
 2. Every application for issue of a license shall be accompanied by
 - (i) a certification practice statement;
 - (ii) a statement including the procedure with respect to identification of the applicant;
 - (iii) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government; and
 - (iv) such other documents, as may be prescribed by the Central Government.

Question 4

XYZ Industries Ltd., a company engaged in a business of manufacturing and supply of electronic equipments to various companies in India. It intends to implement E-Governance system at all of its departments. A system analyst is engaged to conduct requirement analysis and investigation of the present system. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate and reliable. The company is relying on Information Technology for information and transaction processing. It is also presumed that the company is up and running all the time on 24 x 7 basis. Hence, the company has decided to implement a real time ERP package, which equips the enterprise with necessary capabilities to integrate and synchronise the isolated functions into streamlined business processes in order to gain a competitive edge in the volatile business environment. Also, the company intends to keep all the records in digitized form.

- (a) *What do you mean by system requirement analysis? What are the activities to be performed during system requirement analysis phase?*
- (b) *What are the business risks that an organization faces when migrating to real time integrated ERP system?*
- (c) *What are the points that need to be taken into account for the proper implementation of physical and environmental security in respect of Information System Security?*
- (d) *What is the provision given in Information Technology (Amended) Act 2008 for the retention of electronic records?*

Answer

- (a) System requirements analysis is a phase, which includes a thorough and detailed understanding of the current system, identification of the areas that need modification/s

to solve the problem, the determination of user/managerial requirements and to have fair ideas about various system development tools.

The following activities 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 requirements in terms of various parameters like completeness, consistency, unambiguous, verifiable, modifiable, testable and traceable;
 - To gather data or find facts using tools like- interviewing, research/document collection, questionnaires, observation;
 - To develop models to document Data Flow Diagrams, E-R diagrams; and
 - To document activities such as interviews, questionnaires, reports etc. and development of a system dictionary to document the modeling activities.
 - The document/deliverable of this phase is a detailed system requirements report, which is generally termed as SRS.
- (b) Organizations face several business risks when migrating to real-time, integrated ERP systems. These risks are given as follows:
- *Single point of failure*: Since all the organization's data and transaction processing is within one application system, single point failure may be a major risk.
 - *Structural changes*: Significant personnel and organizational structure changes associated with reengineering or redesigning business processes may pose a big challenge.
 - *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 are also great risks.
 - *Online, real-time*: An online real-time environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring re-entry of information.
 - *Change management*: 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.
 - *Distributed computing experience*: Inexperience with implementing and managing distributed computing technology may pose significant challenges.

1.10 Information Systems Concepts

- *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 that 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 exposure 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 a small fraction of the entire ERP's functionality in a particular core module.
- (c) For the proper implementation of Physical and Environmental Security, the following points need to be 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 be securely locked away, when they are not in use.
 - Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to the systems.
 - Supplies and equipments 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 rooms must be away from, and protected against threats of unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

(d) **Retention of Electronic Records: [Section 7] of ITAA 2008** : The provision for the retention of electronic records is discussed in Section 7 of ITAA 2008, which is given as follows:

- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, –
 - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
 - (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format, which can be demonstrated to represent accurately the information originally generated, sent or received;
 - (c) The details, which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record.

However,

this clause does not apply to any information, which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents records or information in the form of electronic records, publication of rules, regulation etc. in Electronic Gazette.

Question 5

ABC Technologies Ltd. is in the development of web applications for various domains. For the development purposes, the company is committed to follow the best practices suggested by SDLC. A system development methodology is a formalized, standardized, 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) *Describe accountants' involvement in development work in brief.*
- (b) *'Waterfall approach is one of the popular approaches for system development'. Explain the basic principles of this approach.*
- (c) *Briefly describe major characteristics of Agile Methodology.*

Answer

- (a) **Accountants' involvement in Development work** : Most accountants are uniquely qualified to participate in systems development because they may be among the few

1.12 Information Systems Concepts

people in an organization who can combine knowledge of IT, business, accounting, and internal control, as well as behavior and communications, to ensure that new systems meet the needs of the user and possess adequate internal controls. They have specialized skills - such as accounting and auditing - that can be applied to the development project. For example, an accountant might perform the analysis of a proposed system's costs and benefits.

(b) Basic Principles of Waterfall Approach

- Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

(c) Some of the Characteristics of Agile Methodology are as follows:

- Iterative with short cycles enabling fast verifications and corrections;
- Time bound iterative cycles;
- Modularity at development process level;
- People oriented;
- Collaborative and communicative working style; and
- Incremental and convergent approach that minimizes risks and facilitates functional additions.

Question 6

XYZ Associates is dealing in the information systems audit and particularly deals with the auditing of controls. Controls are defined as "The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected". The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected. This is achieved by designing an effective information control framework, which comprise policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved.

Read the above carefully and answer the following:

- (a) *Explain the aspects to consider while reviewing the organizational and management controls in an information system.*

- (b) Discuss data processing controls in brief.
- (c) Briefly discuss auditors' role in application software acquisition/selection process.
- (d) What are the costs involved in the implementation and operation of the controls?

Answer

- (a) The controls to consider while reviewing the organizational and management controls in an Information system include:

- .. *Responsibility:* The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.
- .. *An official IT structure:* There should be a prescribed organization structure with all staff deliberated on their roles and responsibilities by written down and agreed job descriptions.
- .. *An IT steering committee:* The steering committee shall comprise of user representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems, for example, the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.

- (b) Data processing controls are given as follows:

- .. *Run-to-run totals:* These help in verifying data that is subject to process through different stages. If the current balance of an invoice ledger is Rs.150,000 and the additional invoices for the period is of total Rs.20,000 then the total sales value should be Rs.170,000. A specific record (probably the last record) can be used to maintain the control total.
- .. *Reasonableness verification:* Two or more fields can be compared and cross verified to ensure their correctness. For example, the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.
- .. *Edit checks:* Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.
- .. *Field initialization:* Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e., setting all values to zero before inserting the field or record.
- .. *Exception reports:* Exception reports are generated to identify errors in data processed. Such exception reports give the transaction code and why the particular transaction was not processed or what is the error in processing the transaction. For example, while processing a journal entry if only debit entry was updated and the credit entry was not up dated due to absence of one of the important fields, then the

1.14 Information Systems Concepts

exception report would detail the transaction code, and why it was not updated in the database.

- .. *Existence/Recovery Controls:* The check-point/restart logs, facility is a short-term backup and recovery control that enables a system to be recovered if failure is temporary and localized.

(c) Auditors' role in application software acquisition/selection process is given as follows:

- .. To highlight risks before a vendor contract or a software agreement contract is signed.
- .. Ensure that the decision to acquire software should flow from the thorough feasibility study, vendor evaluation and RFP (Request for proposal) adequacy checked for.
- .. A RFP would include transaction volume, data base size, turnaround time and response time requirements and vendor responsibilities.
- .. The auditor needs to also check the criteria for pre-qualification of vendors and sufficient documentation available to justify the selection of the final vendor / product.
- .. The auditor may also collect information through his own sources on vendor viability, support infrastructure, service record and the like.
- .. Thorough review of the contract signed with the vendor for adequacy of safeguards and completeness. The contract should address the contingency plan in case of vendor failures such as, source code availability and third party maintenance support.
- .. To ensure that the contract went through legal scrutiny before it was signed.

(d) Implementation and operation of controls in a system involves the following five costs:

- (i) *Initial setup cost:* This cost is incurred to design and implement controls. For example, a security specialist must be employed to design a physical security system.
- (ii) *Executing cost:* This cost is associated with the execution of a control. For example, the cost incurred in using a processor to execute input validation routines for a security system
- (iii) *Correction costs:* The control has operated reliably in signalling an error or irregularity, the cost associated with the correction of error or irregularity.
- (iv) *Failure cost:* The control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses.
- (v) *Maintenance costs:* The cost associated in ensuring the correct working of a control. For example, rewriting input validation routines as the format of input data changes.

Question 7

PQR Enterprises is engaged in a business of manufacturing of electronic products. 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. Basically, risk assessment seeks to identify 'which business processes and related resources are critical to the business', 'what threats or exposures exists, that can cause an unplanned interruption of business processes', and 'what costs accrue due to an interruption'. There are various analytical procedures that are used to determine various risks, threats, and exposures, faced by an organization. These are known as Business Impact Analysis (BIA), Risk Impact Analysis (RIA) and so on.

Read the above carefully and answer the following:

- (a) Define Systematic Risks and Unsystematic Risks with the help of examples.*
- (b) There are various techniques that are available to assess and evaluate risks, namely, Judgement and Intuition, Delphi Approach, Scoring, Qualitative Techniques, and Quantitative Techniques. Explain Delphi and Scoring approaches in brief.*
- (c) In automation of the business modules, retention of electronic records is an important activity. How Information Technology (Amendment) Act 2008 addresses this issue with reference to its Section 7?*

Answer

- (a) Systematic risks:** These are unavoidable risks; constant across majority of technologies and applications. For example the probability of power outage is not dependant on the industry but is dependant on external factors. Systematic risks would remain, no matter what technology is used. Thus effort to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Systematic risks can be reduced by designing management control process and does not involve technological solutions. For example, the solution to non availability of consumable is maintaining a high stock of the same. Thus a systematic risk can be mitigated not by technology but by management process. Hence, one would not make any additional payment for technological solution to the problem. To put in other words there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

Unsystematic risks: These are the risks, which are peculiar to the specific applications or technology. One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system. For example one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. Thus by making additional investment one can mitigate these unsystematic risks.

- (b) **Delphi Approach:** This approach 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.

Scoring Approach: 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.

(c) **[Section 7] Retention of Electronic Records:**

- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
 - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
 - (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
 - (c) the details, which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

However,

This clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules, regulation etc. in Electronic Gazette.

Question 8

ABC Group of Industries is in the process of launching a new business unit, ABC Consultants Ltd. to provide various consultancy services to the organizations worldwide, to assist them in the computerization of their business modules. It involves a number of activities starting from the capturing of the requirements to the maintenance. 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.

Read the above carefully and answer the following:

- (a) What are the issues, which are emphasized by the methodology for developing a business continuity plan?
- (b) Explain the objectives of performing Business Continuity Planning tests.
- (c) What are the issues, written in a contract that should be ensured by security administrators if a third-party site is to be used for backup and recovery purposes?

Answer

- (a) The methodology for developing a business continuity plan emphasizes on the following:
 - (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
 - (ii) Obtaining commitment from appropriate management to support and participate in the effort;
 - (iii) Defining recovery requirements from the perspective of business functions;
 - (iv) Documenting the impact of an extended loss to operations and key business functions;
 - (v) Focusing appropriately on disaster prevention and impact minimization, 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.
- (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.

1.18 Information Systems Concepts

- 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.
 - the success or failure of the business continuity training program is monitored.
- (c) If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as:
- how soon the site will be made available subsequent to a disaster,
 - the number of organizations that will be allowed to use the site concurrently in the event of a disaster,
 - the priority to be given to concurrent users of the site in the event of a common disaster,
 - the period during which the site can be used,
 - the conditions under which the site can be used.
 - the facilities and services the site provider agrees to make available, and
 - what controls will be in place and working at the off-site facility.

Question 9

XYZ Ltd. is a leading company in FMCG sector and has a large number of coffee chains across India. The company uses ERP system for all its business operations and for recording sales at each outlet. The company has customized ERP, which is connected to a central server. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate, it is reliable and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up and running all the time on 24×7 basis. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before.

Read the above carefully and answer the following:

- (a) *An ERP system is not only the integration of various organization processes. Any system has to possess few key characteristics to qualify for a true ERP solution. What are these features?*
- (b) *'Access Control plays a key role in the implementation of information security policies'. Explain its detailed control and objectives.*
- (c) *Describe 'Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security' with respect to the Section 69B of Information Technology (Amendment) Act, 2008.*

- (d) Briefly explain the tasks that are to be performed during the post-implementation period of an ERP package.

Answer

(a) To qualify for a true ERP solution, a system has to possess the following features:

- **Flexibility:** An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).
- **Modular & Open:** ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.
- **Comprehensive:** It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.
- **Beyond The Company:** It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.
- **Best Business Practices:** It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organization.

(b) The detailed control and objectives of access control 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.

(c) [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

1.20 Information Systems Concepts

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.
- (d) Major tasks that are to be performed during the post-implementation of an ERP package are given as follows:
- To develop the new job descriptions and organization structure to suit the post ERP scenario;
 - To determine the skill gap between existing jobs and envisioned jobs;
 - To assess training requirements, and create and implement a training plan;
 - To develop and amend HR, financial and operational policies to suit the future ERP environment; and
 - To develop a plan for workforce logistics adjustment.

Question 10

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, 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 cohesion and coupling with reference to the software designing.*

Answer

- (a) A feasibility study is carried out by the system analysts, which 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.