

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? (10 Marks)*
- (b) The company is advised that the adoption of BS7799 International Standard will help in overcoming the problems and achieving its goals. Discuss. (5 Marks)*
- (c) How should the human resources be enriched for effective utilization of the proposed new systems and standards? (5 Marks)*

(Nov 2009)

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.

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.

- (a) What are the two primary methods through which the analyst would have collected the data ? (5 Marks)
 - (b) To achieve their objectives, what are the points BS 7799 has to ensure ? (5 Marks)
 - (c) Suppose an audit policy is required, how will you lay down the responsibility of audit? (5 Marks)
 - (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? (5 Marks)
- (May 2010)

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.
 - (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?* (5 Marks)
- (b) *What are the types of operations into which the different office activities can be broadly grouped under office automation systems?* (5 Marks)

- (c) *What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity.* (5 Marks)
- (d) *What is the procedure to apply for a license to issue electronic signature certificates, under Section 22, Information Technology (Amendment) Act, 2008?* (5 Marks)
- (Nov 2010)

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.
- (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? (5 Marks)
- (b) What are the business risks that an organization faces when migrating to real time integrated ERP system? (5 Marks)
- (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? (5 Marks)
- (d) What is the provision given in Information Technology (Amended) Act 2008 for the retention of electronic records? (5 Marks)

(May, 2011)

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.
- .. *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.