Questions Based on the Case Studies

Question 1

PQR University is a public university; especially known for its Faculty of Commerce and Management in the country. The faculty offers various UG and PG programs along with research studies viz. M. Phil and Ph.D. Recently, the Academic Council of the university approved the proposal of the faculty to start some UG and PG courses in distance learning mode too. It is observed that the students of distance education are normally dependent on self-study only along with a little support from the concerned department/s. In view of this aforementioned fact, the concerned Dean of the faculty decided to launch a web based Knowledge Portal to facilitate the students of different courses. It is proposed to upload the Study Materials, e-lectures, Suggested Answers of last examinations, Mock Test Papers relevant for the coming examinations etc. of the approved courses on this Knowledge Portal. It is expected that the portal will be very useful for the students as it aims to provide the access of various academic resources on anytime anywhere basis. For the implementation of this project, a technical consultant was appointed by the university. Accordingly, an initial feasibility study under various dimensions was done and a detailed report was submitted. As a next step, as per the recommendations of the consultant, an expression of interest was published by the University in various national/regional newspapers inviting various organizations to showcase their capabilities and suggest a good solution as per the requirements of the concerned faculty of the university.

Read the above carefully and answer the following:

(a) What are three major attributes of information security? Out of these attributes, which attribute will be having the highest priority while developing web based knowledge portal?

(b) What may be the possible dimensions under which the feasibility study of the proposed Knowledge Portal was done in your opinion?

(c) What may be the major validation methods for validating the vendors' proposal for developing the Knowledge Portal?

Answer

(a) Three major attributes of information security are given as follows:

- **Confidentiality:** It refers to the prevention of unauthorized disclosure of information.
- **Integrity:** It refers to the prevention of unauthorized modification of information.
- **Availability:** It refers to the prevention of unauthorized withholding of information.

The proposed Knowledge Portal aims to provide the access of various academic resources on anytime anywhere basis. Hence, out of these attributes, the third attribute namely, availability will be having the highest priority while developing web based knowledge portal.

(b) The possible dimensions under which the feasibility study of the proposed Knowledge Portal was done are given as follows:

- **Technical:** Is the technology needed to build and run the portal available?
- **Financial:** Is the solution financially viable? (e.g. revenue from new course vis-à-vis reduction in cost of classrooms / new cost of developing and running portal)
- **Economic:** What is the Return on Investment?
- **Schedule/Time:** Can the system be delivered on time? (e.g. before start of the new academic year)
- **Resources:** Are human resources (faculty) available to develop the solution or are they reluctant to use it?
- **Operational:** How will the solution work?
- **Behavioral:** Is the solution going to bring any adverse or positive effect on quality of work life? (e.g. enable students to pursue studies at their own time and from their own place of stay without having to be on campus; effect on students / their study due to non-interaction with other students and faculty)
- **Legal:** Is the solution valid in legal terms? E.g. considering the requirements specified by University regulators like UGC – University Grants Commission

(c) Major validation methods of validating the vendors' proposal for developing the Knowledge Portal are given as follows:

- **Checklists:** It is the simplest and rather subjective method for validation and evaluation. The various criteria are put into check lists in the form of suitable questions against which the responses of the various vendors are validated. For example,: Support Service Checklists may have parameters like – Performance, System development, Maintenance, Conversion, Training, Back-up, Proximity, Hardware, Software.
- **Point-Scoring Analysis:** Point-scoring analysis provides an objective means of selecting the final system. There are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. Evaluators must consider such issues as the University's needs to operate and maintain the portal, vendor reputations, software costs, user-friendliness for students (who are the customers in this case), and so forth.
- **Public Evaluation Reports**: Several consultancy agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard. This method has been frequently and usefully employed by

several buyers in the past. For those criteria where published reports are not available, however, resort would have to be made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of facts. E.g. Public reports by agencies like Gartner's magic quadrant on systems used by other universities offering online courses may be considered

- **Benchmarking Problem for Vendor's Proposals:** Benchmarking problems for vendors' proposals are sample programs that represent at least a part of the buyer's primary computer work load and include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs. E.g. develop a set of sample requirements of a student and see whether the proposed system is able to effectively and efficiently deliver them. That is, benchmarking problems are oriented towards testing whether a computer system offered by the vendor meets the requirements of the buyer.
- **Test Problems:** Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to download e-lectures (which are large sized files) by students, response time when large number of students login in at the same time, overhead requirements of the operating system in executing multiple user requests, length of time required to execute an instruction, etc. The results, achieved by the machine can be compared and price performance judgment can be made. It must be borne in mind, however that various capabilities to be tested would have to be assigned relative weightage as all requirements may not be equally important.

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, programme modules and draft agreements are all preserved and administered in 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 ISO 27001 for achieving the same.

(a) What are the two primary methods through which the analyst would have collected the data ?

(b) To retain their e-documents for specified period, what are the conditions laid down in Section 7, Chapter III of Information Technology Act, 2000?

Answer

(a) Two primary methods through which the analyst would have collected the data are given as follows:

(**i**) **Reviewing Internal Documents:** The analyst first tries to learn about the organization involved in or affected by the project. For example, the subsidiary's activities based on its business and operation plans. S/he will also examine proposed organization charts and functions of positions mentioned in it.

(ii) 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. The analyst may conduct interviews with persons who are scheduled to occupy various positions in the subsidiary.

(b) Section 7, Chapter III of Information Technology Act, 2000 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:

(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.

E.g. Company may include clause in its contracts with customers that electronic documents and correspondence will be considered valid; Electronic documents will have to be preserved till the contract and all liabilities are discharged; Documents may be digitally signed with hash values to assure that they have not been altered; All correspondence with clients may be saved with dates of transmission / receipt; In case the company changes / upgrades its email or other systems, the new system should be able to read the old data and retain all data without change etc.

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) What are the types of operations into which the different office activities can be broadly grouped under office automation systems?

(b) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity.

Answer

(a) 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 from customers, enquiries, notes, handouts, charts, graphs etc. need to be preserved for being tracked through their life.

(ii) **Document Creation:** This consists of preparation of documents, editing of texts etc. and takes up major part of the time of field personnel like salesmen.

(iii) **Receipts and Distribution**: This basically includes distribution of correspondence to designated recipients. This may be effectively achieved by use of emails and mail groups.

(iv) **Filling, Search, Retrieval and Follow-up:** This is related to filling, indexing, searching of documents, which takes up significant time. E.g. categorizing various types of documents and cataloguing all documents under each type, assigning rights for access, retrieval

(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. Care should be taken to convert old documents which have not been created in or stored in computers into usable electronic documents so that after the new system is implemented, these old documents will still be accessible and business can continue as usual. Office automation systems which are already in use by some departments must be integrated with the new systems.

For e-governance, the company must put in place a definition of road map of how the systems will be implemented, monitored, measured and corrective action taken when deficiencies / opportunities for improvement are noticed. This will include assigning responsibilities to various personnel using or affected by office automation.

(b) 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. It is especially important because the company is planning to embrace office automation in all aspects of business. This will make it highly dependent on computer systems to run operations, deal with customers, suppliers and other stakeholders etc. 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 Operational piece of business continuity planning to resume normal operations after a disaster.

(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. Planning which are minimal level of operations which must be run, their priority and the sequence in which they need to be brought up as well as taking steps to be prepared to deal with any emergency.

(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. E.g. how to run operations and service customers when computer systems, are not available. The major international companies who have given orders to the company will expect this level of preparedness from the company.

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 synchronize 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 is the provision given in Information Technology Act 2000 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 e.g. what facilities the business owners require to gain competitive advantage; whether for meeting 24x7 requirements documents should be accessible over internet, whether customers and suppliers will also connect to the system;
- To analyze requirements to detect and correct conflicts and determine priorities; this will include identifying the various documents which will need to be migrated to the new system. In case the existing systems process transactions in a way different from the new ERP, these differences must be resolved
- 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 develop 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) Retention of Electronic Records: [Section 7] of Information Technology Act 2000: The provision for the retention of electronic records is discussed in Section 7 of IT Act 2000, 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.

E.g. Company may include clause in its contracts with customers that electronic documents and correspondence will be considered valid; Electronic documents will have to be preserved till the contract and all liabilities are discharged; Documents may be digitally signed with hash values to assure that they have not been altered; All correspondence with clients may be saved with dates of transmission / receipt; In case the company changes / upgrades its email or other systems, the new system should be able to read the old data and retain all data without change etc.

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: An accountant can help in various related aspects during system development; some of them are as follows:

(i) Return on Investment (referred as RoI): This calculates the return an entity shall earn on a particular investment i.e. capital expenditure. This financial data is a prime consideration for evaluating any capital expenditure by the entity. The

important data required for this analysis are the cost of implementing and running the project, and the expected revenue/ benefit for a given period. The analysis ideally needs to be done before the start of the development efforts for better decision making by management. For this analysis following data needs to be generated.

(1) Cost: This includes estimates for typical costs involved in the development, which are given as follows:

- **Development Costs:** Development Costs for a computer based information system include costs of the system development process, like salaries of developers, software, equipment depreciation etc.
- **Operating Costs:** Operating Costs of a computer based information system including hardware/ software rental or depreciation charges; salaries of computer operators and other data processing personnel, who will operate the new system.
- **Intangible Costs:** Intangible Costs that cannot be easily measured. For example, the development of a new system may disrupt the activities of an organization and cause a loss of employee productivity or morale.

(2) Benefits: The benefits, which result from developing new or improved information systems can be subdivided into tangible and intangible benefits. A post implementation analysis is also done to see how the system development effort has benefitted an organization. For example: A large oil company in public sector, implemented an ERP system few years back at a total cost of ` 100 crores. The calculated benefits from the project were ` 40 crores per annum. Above data gives an RoI of 40%, which is tremendous for any business. It also tells that the payback period is around 2.5 years.

(ii) Computing Cost of IT Implementation and Cost Benefit Analysis: For analysis of ROI, accountants need the costs and returns from the system development efforts. For correct generation of data, proper accounting needs to be done. Accountants are the persons to whom management look for this purpose.

(iii) Skills expected from an Accountant: An accountant, being an expert in accounting field must possess skills to understand the system development efforts and nuances of the same. S/he is expected to have various key skills, including understanding of the business objectives, expert book keeper, and understanding of system development efforts etc.

(b) Basic Principles of Waterfall Approach: Major principles of Waterfall approach are given as follows:

- 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) Major characteristics of Agile Methodology are as follows:

- Customer satisfaction by rapid delivery of useful software;
- Welcome changing requirements, even late in development;
- Working software is delivered frequently (in weeks rather than months);
- Working software is the principal measure of progress;
- Sustainable development, able to maintain a constant pace;
- Close, daily co-operation between business people and developers;
- Face-to-face conversation is the best form of communication (co-location);
- Projects are built around motivated individuals, who should be trusted;
- Continuous attention to technical excellence and good design;
- Simplicity; Self-organizing teams; and
- Regular adaptation to changing circumstances.

Question 6

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 capturing of requirements to maintenance. Business continuity and disaster recovery planning are two key activities in this entire process, which must be taken care of 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 recovery purposes?

Answer

(a) The methodology for developing a business continuity plan emphasizes 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;

(viii) Planning the testing of plans in a systematic manner and measuring results of such tests; and

(ix) 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.
- the resources such as business processes, IS systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
- manual recovery procedures and IT backup system/s are current and can either be operational or restored.
- the success or failure of business continuity training program is monitored.

(c) If a third-party site is to be used for 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,
- procedures to ensure security of company's data from being accessed / damaged by other users of the facility and
- what controls will be in place for working at the off-site facility.

Question 7

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.

Answer

(a) A feasibility study is carried out by 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 financially viable?
- **Economic:** What is the Return on Investment?
- **Schedule/Time:** Can the system be delivered on time?
- **Resources:** Are human resources available to develop the solution or are they reluctant to use it?

- **Operational:** How will the solution work?
- **Behavioral:** Is the solution going to bring any positive or 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 iteration is rigid and does 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, hence well-defined interfaces are required.
- Difficult problems tend to be pushed to the future to demonstrate early success to management.

Question 8

ABC Ltd. is a company dealing in various computer hardware items through its various offices in India and abroad. By recognizing the advantages of connectivity through internet, recently, the company decided to sell its products in on-line mode also to facilitate its customers worldwide. For development of the company's web applications, the company appointed a technical consultant initially for one year to work on behalf of the company to take the matter forward. The consultant called various meetings of different stakeholders and decided to follow the best practices of SDLC for its different phases. In the current vulnerable world, keeping the importance of information security in view particularly, he further suggested to consider the security issues from the inception itself i.e. starting from the requirements analysis phase till maintenance. Accordingly, efficient ways were also explored to achieve the goals especially for security. Research Studies reveal that cost and efforts may be reduced up to a considerable level by incorporating security from the beginning in the SDLC.

Read the above carefully and answer the following:

(a) What is SDLC? Explain the key activities performed in the Requirements Analysis phase.

(b) Agile methodology is one of the popular approaches of system development. What are the weaknesses of this methodology in your opinion?

Answer

(a) System Development Life Cycle (SDLC) framework provides system designers and developers a sequence of activities to follow. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one. The SDLC

is document driven, which means that at crucial stages during the process, documentation is produced. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced. These are sometimes referred as deliverables.

Key activities, which are performed in the 'Requirements Analysis Phase', are given as follows:

- To identify and consult the stakeholders to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine priorities;
- To verify the requirements to be 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 modeling activities.

(b) Major weaknesses of agile methodology are given as follows:

- In case of some software deliverables, especially the large ones, it is difficult to assess the efforts required at the beginning of the software development life cycle. Hence, appropriate resources may not be available or cost-benefit may be overestimated.
- There is lack of emphasis on necessary design and documentation. This makes maintenance difficult.
- Agile increases potential threats to business continuity and knowledge transfer. By nature, Agile projects are extremely light on documentation because the team focuses on verbal communication with the customer rather than on documents or manuals.
- Agile requires more re-work. Because of the lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects when the various components of the software are combined and forced to interact.
- The project can easily get taken off track if the customer representative is not clear about the final outcome that they want.
- Only senior programmers are capable of taking the kind of decisions required during the development process. Hence, it has no place for newly appointed programmers, unless combined with experienced resources.
- Agile lacks the attention to outside integration. Because Agile teams often do not invest the time in identifying and designing the integration points with other systems in advance, the need for an integration point can become a last-minute surprise that

often requires re-work, additional time, removal from scope, or a poor-quality product.

Question 9

XYZ Limited is a multinational company engaged in providing financial services worldwide. Most of the transactions are done online. Their current system is unable to cope up with the growing volume of transactions. Frequent connectivity problems, slow processing and a few instances of phishing attacks were also reported. Hence the Company has decided to develop a more robust in-house software for providing good governance and sufficient use of computer and IT resources. You, being an IS auditor, has been appointed by the Company to advise them on various aspects of project development and implementation. They want the highest levels of controls in place to maintain data integrity and security with zero tolerance to errors.

The Company sought your advice on the following issues:

(a) What are the major data integrity policies you would suggest?

(b) What are the categories of tests that a programmer typically performs on a program unit?

(c) Discuss some of the critical controls required in a. computerized environment.

(d) What are your recommendations for efficient use of computer and IT resources to achieve the objectives of 'Green Computing'?

Answer

(a) Major data integrity policies are given as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.
- **Offsite Backup Storage:** Backups older than one month must be sent offsite for permanent storage.
- **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes.
- **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

(b) There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows:

- **Functional Tests:** Functional Tests check 'whether programs do, what they are supposed to do or not'. The test plan specifies operating conditions, input values,

and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.

- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
- **Stress Tests:** 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, to observe the results. The purpose of a stress test is to determine the limitations of the program.
- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

(c) Some of the critical controls required in a computerized environment are as follows:

- Management understanding of Information System risks and related controls;
- Presence or adequate Information System control framework;
- Presence of general controls and Information System controls;
- Awareness and knowledge of Information System risks and controls amongst the business users and even IT staff;
- Implementation of controls in distributed computing environments and extended enterprises;
- Control features or their implementation in highly technology driven environments; and
- Appropriate technology implementations or adequate security functionality in technologies implemented.

(d) Some recommendations for efficient use of computer and IT resources to achieve the objectives of 'Green Computing' are as follows:

- Power-down the CPU and all peripherals during extended periods of inactivity.
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times.
- Power-up and power-down energy-intensive peripherals such as laser printers per need.
- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
- Use notebook computers rather than desktop computers whenever possible.

- Use the power-management features to turn off hard drives and displays after several minutes of inactivity.
- Minimize the use of paper and properly recycle waste paper.
- Dispose of e-waste per central, state and local regulations.
- Employ alternative energy sources for computing workstations, servers, networks and data centers.

Question 10

E-quip Limited has worldwide operations and is engaged in the business of manufacturing and supply of electronic equipment through its various outlets in India and abroad. Recognizing the advantages of connectivity through internet, the Management decides to sell its products in on-line mode by using Cloud Computing technology to achieve this objective.

The Company appoints a technical team for the development of the Company's new web application. The team calls for various meetings of different stakeholders and decides to follow the best practices of SDLC for its different phases. Keeping the importance of information security in the current vulnerable world, it suggests that security issues must be considered from the beginning itself. Accordingly, Business Impact Analysis (BIA) was done as a part of Business Continuity Management (BCM). As the auditor member of the technical team, the Management of E-quip Limited wants you to advise them on the following issues:

(a) What are the advantages and important implications of the proposed Information System for the Company?

(b) What are the tasks you will undertake to ensure that BCM program is in place, while assessing BIA?

(c) Management wants to know the major challenges in using Cloud Computing technology for running the new web application. Write any five challenges.

(d) Explain briefly major ways to control remote and distributed data processing in the new Web Application.

Answer

(a) The major advantage of the proposed Information system will be that it will enable the E-quip Limited to sell its products in an online mode in India and abroad through Internet connectivity by using Cloud Computing Technology. The proposed Information system will support company's business processes and operations; better business decision making; and will provide strategic and competitive advantage to ensure better quality and supply of its electronic equipments.

Following are some of the important implications of proposed Information Systems in business for E-Quip Limited:

- Information system helps managers in efficient decision-making to achieve the organizational goals.

- An organization will be able to survive and thrive in a highly competitive environment on the strength of a well-designed Information system.
- Information systems helps in making right decision at the right time i.e. just on time.
- A good information system may help in generating innovative ideas for solving critical problems.
- Knowledge gathered though Information system may be utilized by managers in unusual situations.
- Information system is viewed as a process; it can be integrated to formulate a strategy of action or operation.

(b) Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The tasks to be undertaken to ensure that BCM program is in place while assessing BIA are as follows:

- Assess the impacts that would occur if the activity was disrupted over a period;
- Identify the maximum time after the start of a disruption within which the activity needs to be resumed;
- Identify critical business processes;
- Assess the minimum level at which the activity needs to be performed on its resumption;
- Identify the length of time within which normal levels of operation need to be resumed; and
- Identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

(c) Major challenges in Cloud Computing Technology for running new Web application are as follows:

- **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality. With the use of encryption and physical isolation, data can be kept secret.
- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible.
- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure and natural calamities are all threats to availability.
- **Governance:** Due to the lack of control over the employees and services, there is problem relating to design, implementation, testing and deployment. So, there is a

need of governance model, which controls the standards, procedures and policies of the organization.

- **Trust:** Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.
- **Legal Issues and Compliance:** There are various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements.
- **Privacy:** The privacy issues are embedded in each phase of the Cloud design that includes both the legal compliance and trusting maturity.
- **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'.
- **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. Some of the Cloud providers use server/s from other service providers and thus there is a probability that the data is less secure and is more prone to the loss from external server.
- **Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The reliability and scalability of architecture is dependent on the design and implementation to support the overall framework.
- **Identity Management and Access control:** A robust federated identity management architecture and strategy internal in the organization provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.
- **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
- **Software Isolation:** Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture and evaluate the risks required for the organization.
- **Application Security:** Security issues relating to application security still apply when applications move to a cloud platform. Service provider should have the complete access to the server with all rights for monitoring and maintenance of server.

(d) Remote and distributed data processing applications can be controlled in many ways. Some of these are given as follows:

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

Question 11

XYZ Ecom Ltd, is establishing an e-Commerce platform to enable business to customer (B2C) process online. This platform will offer safe integrated supply process by e-linking suppliers, customers and bankers/payment gateways. The company proposes to keep the systems 24x7 working over internet. Everyone concerned will be first registered with the databases of the company. All the data shall be stored across servers on internet based cloud environment in a secured manner.

Read the above carefully and answer the following:

(a) If the employees of the company can use personal devoices such a laptop smartphones, tablets etc. to connect and access the data, what could be the security risks involved? Classify and elaborate such risks.

(b) What are the advantages of using cloud computing environment?

(c) In this company, what are your functions as an IS auditor?

(d) List and explain the advantages of using continuous audit techniques for the proposed system.

Answer

(a) The policy under which the employees of the company are allowed using Personal devices such as laptop, smart phones, tablets etc. to connect to the corporate network to access information and application is known as BYOD (Bring Your Own Device) policy.

Under this, there will be certain amount of risk associated with the client's data, which can be classified into four areas given below:

- **Network Risks:** Under BYOD; when employees carry their own devices to workplace (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the company's network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need to be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.
- **Device Risks:** A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threat.
- **Application Risks:** When most employees' phones and smart devices are connected to the corporate network that are not protected by security software, probability of concurrent mobile vulnerabilities increase. Organizations become unclear in deciding that 'who is responsible for device security – the organization or the user'.
- **Implementation Risks:** Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above-mentioned threats.

(b) Major advantages of Cloud Computing environment are given below:

- **Cost Efficiency:** Cloud computing is probably the most cost efficient method to use, maintain and upgrade. The cloud is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.
- **Almost Unlimited Storage:** Storing information in the cloud gives us almost unlimited storage capacity. Hence, one does not need to worry about running out of storage space or increasing the current storage space availability.
- **Backup and Recovery:** Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

- **Automatic Software Integration:** In the cloud, software integration is usually automatic wherein no additional efforts are taken to customize and integrate the applications as per our preferences and with great ease. Hence, one can handpick just those services and software applications that s/he thinks will best suit his/her enterprise.
- **Easy Access to Information:** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.
- **Quick Deployment:** Cloud computing gives us the advantage of quick deployment. Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes.

(c) Information System Auditor often is the assessor of business risk, as it relates to the use of IT, to management. The auditor can check the technicalities well enough to understand the risk (not necessarily manage the technology) and make a sound assessment and present risk-oriented advice to management.

As an IS Auditor, we would review majorly the risks relating to IT systems and processes; some of which are as follows:

- Inadequate information security controls (e.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.)
- Inefficient use of resources, or poor governance (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.)
- Ineffective IT strategies; policies and practices (including lack of policies for use of Information and Communication Technology (ICT) resources; Internet usage policies; and Security practices etc.)
- IT-related frauds (including phishing; and hacking etc.)

(d) Some of the advantages of using continuous audit techniques for the proposed system are as under:

- **Timely, Comprehensive and Detailed Auditing:** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
- **Surprise test capability:** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives:** Continuous audit techniques provides information to systems staff regarding the test vehicle to be

used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.

- **Training for new users:** Using the Integrated Test Facilities (ITFs), new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

Question 12

Bharat Bank (BB) is a large bank with more than 3000 branches and 15000 ATMS in India. With an aim to grow further, it has acquired three smaller private banks with similar lunes of business. This acquisition has brought a variety of products, applications and branches under its umbrella. Besides consumer banking through brick and mortar branches, BB also wants to consolidate its position through internet banking.

The growth strategy of the bank has resulted in fragmented business operations that operate in a regional structure as well as a disjoint IT environment. Hence BB wishes to implement a new, cutting edge web-based Core Banking System to manage all its operations from a single window. BB also recognizes that failure or malfunction pf any critical system will cause significant operational disruptions and materially impact its ability to provide service to its customers. To overcome this risk, BB plans to implement Business Continuity Management (BCM). You have been appointed by BB to make a presentation to the Board of Directors to justify the need for the new system. Please answer the following queries raised by the Management:

(a) What are the key management practices which are required for aligning IT strategy of BB with its enterprise Strategy?

(b) What are the IT tools you consider critical for business growth?

(c) What are the suggested system controls that should be covered under IS audit as per the requirement of the Reserve Bank of India?

(d) Explain the five stages or components of the BCM process which will help BB to manage any future disruptions of the proposed new Core Banking System.

Answer

(a) The key management practices which are required for aligning IT strategy of Bharat Bank (BB) with its enterprise strategy are as follows:

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to

IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.

- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

(b) Some of the IT tools critical for business growth are as follows:

- **Business Website –** By having a website, enterprise/business becomes reachable to large number of customers. In addition, it can also be used in an advertisement, which is cost effective and in customer relationship management.
- **Internet and Intranet –** Through Internet, time and space are no obstacles for conducting meeting of people working in a team from multiple locations, or with different vendors and companies. Intranet is system that permits the electronic exchange of business data within an organization, mostly between managers and senior staff. E-commerce among partners (suppliers, wholesalers, retailers, distributors) using intranets, e-mail etc. provides new platform to the business world for conducting business in a faster and easier way.
- **Software and Packages** – DBMS, data warehousing, data mining tools, knowledge discovery can be used for getting information that plays important role in decision making that can boost the business in the competitive world. ERP is one of the

latest high-end solutions that streamlines and integrates operation processes and information flows in the company to synergize major resources of an organization.

- **Business Intelligence –** Business Intelligence (BI) refers to applications and technologies that are used to collect; provide access and analyze data and information about company's operations. Some BI applications are used to analyze performance or internal operations e.g. EIS (Executive Information System), business planning, finance and budgeting tools; while others are used to store and analyze data e.g. Data mining, Data Warehouses, Decision Support System etc. Some BI applications are also used to analyze or manage the human resources e.g. customer relationship and marketing tools.
- **Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc**. - Webcam, microphone etc. are used in conducting long distance meeting. Use of computer systems, printer, and scanner increases accuracy, reduce processing times, enable decisions to be made more quickly and speed up customer service.

(c) The System Controls that should be covered under the Information Systems' audit as per the requirement of the Reserve Bank of India (RBI) are as follows:

- Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming/design. System person would only make modifications/ improvements to programs and the operating persons would only use such programs without having the right to make any modifications.
- Contingency plans/procedures in case of failure of system should be introduced/ tested at periodic intervals. EDP auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.
- An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements.
- To bring about uniformity of software used by various branches/offices, there should be a formal method of incorporating change in standard software and it should be approved by senior management. Inspection and Audit Department should verify such changes from the view-point of control and for its implementation in other branches to maintain uniformity.
- Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.
- There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.
- With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the banks Internal Audit including IS Audit to validate the approach and practices

adopted by them in the discharge of its responsibilities as laid out in the Audit Charter/Audit Policy.

(d) The stages or components of the BCM process which will help Bharat Bank (BB) to manage any future disruptions of the proposed new Core Banking system are as follows:

- **Stage 1: BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
- **Stage 2: BCM – Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. The selection of strategy will consider the processes and technology already present within the enterprise.
- **Stage 3: BCM – Development and Implementation Process:** This deals with the development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
- **Stage 4: BCM – Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and identifies opportunities for improvement.
- **Stage 5: BCM – Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

Question 13

ABC limited is a reputed Insurance company with their head office located in Chicago. With an aim to expand their business, they started a subsidiary company in India and obtained the license from IRDA. Now they want to set-up branches throughout India and to appoint agents to sell their Insurance Products. The company want to use latest technologies and to establish an IT Department with full IS security. The company was to implement COBIT 5 in their organization. Further they also want to sell their insurance products online and to develop a website to provide E-Commerce facility and implement Mobile Computing in their company. You are appointed as IT Consultant for this company. Please answer the following queries raised by the Management?

(a) What are the enablers described by COBIT 5 Framework?

(b) What are the limitations of mobile computing?

(c) What is the information that an IS Auditor is expected to obtain at the audit location before proceeding with the IS Audit as per the provisions of IRDA?

(d) Explain the Impact of Cyber Frauds on Enterprises.

Answer

(a) The COBIT 5 framework describes seven categories of enablers which are as follows:

- ***Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.*
- ***Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.*
- ***Organizational structures** are the key decision-making entities in an enterprise.*
- ***Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.*
- ***Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.*
- ***Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.*
- ***Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.*

(b) Limitations of Mobile Computing are as follows:

- ***Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and Enhanced Data for GSM (Global System for Mobile Communication) Evolution (EDGE), and more recently 3G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.*
- ***Security Standards:** When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards. One can easily attack the VPN through a huge number of networks interconnected through the line.*

- ***Power consumption:*** *When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life. Mobile computing should also look into Greener IT in such a way that it saves the power or increases the battery life.*
- ***Transmission interferences:*** *Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.*
- ***Potential health hazards:*** *People who use mobile devices while driving is often distracted from driving are thus assumed to be more likely involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.*
- ***Human interface with device:*** *Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.*

(c) Before proceeding with the Information Systems Audit as per the provisions of IRDA (Insurance Regulatory and Development Authority of India), an IS auditor is expected to obtain the following information at the audit location:

- *Location(s) from where Investment activity is conducted.*
- *IT Applications used to manage the Insurer's Investment Portfolio.*
- *Obtain the system layout of the IT and network infrastructure including: Server details, database details, type of network connectivity, firewalls other facilities/ utilities.*
- *Are systems and applications hosted at a central location or hosted at different office?*
- *Previous Audit reports and open issues / details of unresolved issues from Internal Audit, Statutory Audit, and IRDA Inspection / Audit.*
- *Internal circulars and guidelines of the Insurer.*
- *Standard Operating Procedures (SOP).*
- *List of new Products/funds introduced during the period under review along with IRDA approvals for the same.*
- *Scrip-wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.*
- *IRDA Correspondence files, circulars and notifications issued by IRDA.*
- *IT Security Policy.*

- *Business Continuity Plans.*
- *Network Security Reports pertaining to IT Assets.*

(d) The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- *<u>Financial Loss:</u> Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.*
- *<u>Legal Repercussions:</u> Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology (Amendment) Act 2008, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.*
- *<u>Loss of credibility or Competitive Edge:</u> News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility. There have been instances where share prices of such companies went down, as the news of such attack percolated to the market.*
- *<u>Disclosure of Confidential, Sensitive or Embarrassing Information:</u> Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.*
- *<u>Sabotage:</u> The above situation may lead to misuse of such information by enemy country.*

Question 14

ABC Limited, a large enterprise with more than 12000 employees, plans to implement an MIS to support middle and senior level management in administration and decision making. As an expert, what would be your response to the following:

(a) Major limitations of a Management Information System.

(b) Important implications of an MIS in business.

(c) What are the categories of system maintenance?

(d) What are the major aspects to be looked into by an IS Auditor?

Answer

(a) Major Limitations of Management Information Systems (MIS) are as follows:

- *The quality of the outputs of MIS is basically governed by the quality of input and processes.*
- *MIS is not a substitute for effective management, which means that it cannot replace managerial judgment in making decisions in different functional areas. It*

is merely an important tool in the hands of executives for decision making and problem solving.

- *MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.*
- *MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.*
- *MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives or senior management.*
- *MIS is less useful for making non-programmed decisions. Such types of decisions are not of the routine type and thus require information, which may not be available from existing MIS to executives.*
- *The effectiveness of MIS is reduced in enterprises, where the culture of hoarding information and not sharing with other holds.*
- *MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.*

(b) Following are some of the important implications of Management Information Systems (MIS) in business:

- *MIS supports the managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill the organizational goals.*
- *An organization can survive and thrive in a highly competitive environment on the strength of a well-designed Management Information system that provides flexible and speedy access to accurate data.*
- *MIS helps in making right decision at the right time i.e. just on time.*
- *A good MIS may help in generating innovative ideas for solving critical problems.*
- *Knowledge gathered though MIS may be utilized by managers in unusual situations.*
- *MIS may be viewed as a process; it can be integrated to formulate a strategy of action or operation.*
- *MIS provides reports to management that can help in making effective, structured types as applicable to decisions of day-to-day operations.*

(c) System Maintenance can be categorized in the following ways:

- *<u>Scheduled Maintenance:</u> Scheduled Maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For*

example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.

- ***Rescue Maintenance:*** *Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.*
- ***Corrective Maintenance:*** *Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.*
- ***Adaptive Maintenance:*** *Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.*
- ***Perfective Maintenance:*** *Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.*
- ***Preventive Maintenance:*** *Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.*

(d) The major aspects that an Information Systems (IS) Auditor must consider while implementing an MIS in a large enterprise ABC Limited, to support middle and senior level management in administration and decision making are as follows:

An auditor must –

- *Assess the extent to which the system being developed provides for adequate audit trails and controls to ensure the integrity of data processed and stored;*
- *Ensure 'what project control standards are to be complied with' and determining the extent to which compliance is being achieved;*
- *Examine system documentation such as functional specifications to arrive at an opinion on controls;*
- *Provide a list of the standard controls, over operational concerns such as response time, CPU usage, and random access space availability that he/she can use as an assessment criteria;*

- *Review Feasibility Study Report and different work products of the Feasibility study phase;*
- *Include technical experts to seek their opinion on the technical aspects of development of MIS;*
- *Give control objectives, directives and in general, validate the opinion expressed by technical experts;*
- *Review some of the control considerations like –*
    - *Documented policy and procedures;*
    - *Established Project team with all infrastructure and facilities;*
    - *Developers/ IT managers are trained on the procedures;*
    - *Appropriate approvals are being taken at identified mile-stones;*
    - *Development is carried over as per standards, functional specifications;*
    - *Separate test environment for development/ test/ production / test plans;*
    - *Design norms and naming conventions are as per standards and are adhered to;*
    - *Business owners testing and approval before system going live; Version control on programs;*
    - *Source Code is properly secured;*
    - *Adequate audit trails are provided in system; and*
    - *Appropriateness of methodologies selected.*

Question 15

XYZ Appliances Ltd., is a popular marketing company, which has branches in any locations. It does all its business activities on-line such as exchanging information relating to the buying and selling of goods, distribution information and providing customer support. With the increase in business activities and increase in regulations, the company is facing several problems with its existing information system. It realizes that the existing Information System has to be improved and proper controls have to be incorporated. It wishes to enhance the existing Information System and put in sufficient measures to ensure security of data and protect the company against breaches caused by security failures. The company has decided to use a third-party site for backup and recovery procedures. To develop the new system the company formed a full-fledged System Development team. The team followed all the phases in the SDLC and implemented the new system successfully.

The company was also satisfied with the post-implementation audit report. Answer the following questions based on the above:

(a) As a system development team member, explain the areas that should be studied in depth to understand the present system.

(b) Discuss the activities that deal with the Systems Development Management Controls in the IT set-up.

(c) What are the issues that the security administrators should consider when drafting the contract with a third party for a backup and recovery site?

(d) As an IS auditor, how do you evaluate the performance of the following Managerial Controls:

(i) Data Resource Management Controls and

(ii) Security Management Controls.

Answer

(a) As a System development team member, following areas should be studied to understand the present system:

- *Reviewing Historical Aspects: The historical facts of an organization enable the system analyst to identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate 'what system changes have occurred in the past including operations' that have been successful or unsuccessful with computer equipment and techniques.*
- *Analyzing Inputs: A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of various sources from where the data are initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, 'what is contained in it', 'who prepared it', 'from where the form is initiated', 'where it is completed', the distribution of the form and other similar considerations.*
- *Reviewing Data Files: The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval, these are used. Information on common data files and their size will be an important factor, which will influence the new information system. The system analyst should also review all on-line and off-line files, which are maintained in the organization as it will reveal information about data that are not contained in any outputs.*

- ***Reviewing Methods, Procedures and Data Communications:*** *Methods and procedures transform input data into useful output. A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system. A system analyst also needs to review and understand the present data communications used by the organization. S/he must review the types of data communication equipment including data interface, data links, modems, dial-up and leased lines and multiplexers. The system analyst must understand how the data-communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.*
- ***Analyzing Outputs: The*** *outputs or reports should be scrutinized by the system analysts in order to determine "how well they will meet the organization's needs". The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting is used, how long it is kept on file, etc. must be investigated.*
- ***Reviewing Internal Controls:*** *A detailed investigation of the present information system is not complete until internal control mechanism is reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipment might allow much greater control over the data.*
- ***Modeling the Existing System:*** *As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the processes must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps to disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.*
- ***Undertaking Overall Analysis of the Existing system:*** *Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of the present work volume; the current personnel requirements; the present costs-benefits of each of these must be investigated thoroughly.*

(b) The activities that deal with Systems Development Management Controls in the IT setup are as follows:

- ***System Authorization Activities:*** *All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.*
- ***User Specification Activities:*** *Users must be actively involved in the systems development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals.*
- ***Technical Design Activities:*** *The technical design activities in the Systems Development Life Cycle (SDLC) translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase.*
- ***Internal Auditor's Participation: The*** *internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.*
- ***Program Testing:*** *All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors. To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use. This will give the auditor a frame of reference for designing and evaluating future audit tests*
- ***User Test and Acceptance Procedures:*** *Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s). The formal test and acceptance of the system should consider being the most important control over the SDLC.*

(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?*

(d) (i) To evaluate the performance of Data Resource Management Controls under Managerial Controls, an IS Auditor -

- *Should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls.*
- *Might employ test data to evaluate whether access controls and update controls are working.*

(ii) To evaluate the performance of Security Management Controls under Managerial Controls, an IS Auditor -

- *must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;*
- *checks whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and*
- *Checks whether the organizations have opted for an appropriate insurance plan or not.*

Question 16

ABC Corporation desires to implement an Expert System to manage suspicious transactions, financial forecast, etc. to facilitate informed decision making, by various stake holders of the corporation. You have been appointed as IT manager to setup domain-specific and high quality knowledge based system and to enhance internal controls to maintain data integrity and security. Moreover, to help managers in making better decisions, the company decided to develop and implement Information System following System Development Life Cycle (SDLC) approach of system development. The top management of the Corporation is seeking your views on the following issues to be explained in brief:

(a) Some of the business application areas of Expert System.

(b) Knowledge areas required by a business manager to operate Information System in effective and efficient manner.

(c) Interrelated components of internal controls

(d) Various evaluation methods in post implementation review in respect to user satisfaction with the Information System.

Answer

(a) Some of the business application areas of Expert Systems are as follows:

- *Accounting and Finance - It provides tax advice and assistance, helping with credit- authorization decisions, selecting forecasting models, providing investment advice.*
- *Marketing - It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.*
- *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.*
- *Personnel - It is useful in assessing applicant qualifications and assisting employees in filling out forms.*
- *General Business - It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, and evaluating performance.*

(b) To operate Information Systems (IS) effectively and efficiently, a business manager should have knowledge in the following areas:

- *Foundation Concepts – It includes fundamental business and managerial concepts e.g. 'what are components of a system and their functions', or 'what competitive strategies are required'.*
- *Information Technologies (IT) – It includes operation, development and management of hardware, software, data management, networks and other technologies.*
- *Business Applications – It includes major uses of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.*
- *Development Processes – It comprises how end users and Information Systems specialists develop and execute business/IT solutions to problems.*

- ***Management Challenges** – It includes 'how the function and IT resources are maintained' and utilized to attain top performance and build the business strategies.*

(c) Internal Control is comprised of following five interrelated components:

- ***Control Environment:** This includes the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on. For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.*
- ***Risk Assessment:** This includes the elements that identify and analyse the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation. Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.*
- ***Control Activities:** This includes the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.*
- ***Information and Communication**: These are the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities. These are associated with control activities regarding information and communication systems of the entity that acts as one of the components of internal accounting system. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.*
- ***Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions. This includes the elements that ensure internal controls operate reliably over time. The best internal controls are worthless if the company does not monitor them and make changes when they are not working.*

(d) Various evaluation methods in post-implementation review in respect to user satisfaction with the Information System include the following:

- *Development Evaluation: Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained. However, it may be noted that very few information systems have been developed on schedule and within budget. In fact, many information systems are developed without clearly defined schedules or budgets. Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.*
- *Operational Evaluation: The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties. It tries to answer the questions related to functional aspects of the system. Such an evaluation is relatively straightforward if evaluation criteria are established in advance. For example, if the systems analyst lays down the criterion that a system, which can support one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.*
- *Information Evaluation: An information system should also be evaluated in terms of information it provides or generates. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operational evaluations. The objective of an information system is to provide information to a considerable extent to support the organizational decision system. Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system.*

Question 17

The XYZ Company is marketing several household consumable products. It has several branches throughout the country, which are well-connected with internet and intranet. Based on the reports and feedbacks, the company understands that the present system is not able to meet the requirements of its IS stakeholders. Hence, it wants to improve it's IS performance and availability of services, to minimize its loss in terms of revenue loss, loss of reputation and to improve the customer satisfaction. It has felt the need for having reengineered business processes and implementing BCM for assessing the potential threats and managing the consequences. It wants to ensure to provide all users with a secure Information Processing environment. Further it wants to provide continuous assurance about the quality of data by employing continuous auditing technique SCARF. Hence, it engages a highly professional System Development Team

to study the present system for designing and implementing a new system. The team follows and takes advantages of SDLC methods.

Read the above carefully and being a member of the team, answer the following:

(a) Briefly discuss the steps that involved in Business Process Design.

(b) Discuss the means for achieving Network Access Controls.

(c) Discuss:

(i) as to how an enterprise uses Training Process as a tool to initiate a culture of BCM in all the stakeholders and

(ii) what supports are needed for the development of a BCM culture.

(d) Discuss the types of information that can be collected by SCARF.

Answer

(a) Business Process Design involves a sequence of the steps described briefly below:

(i) <u>Present Process Documentation:</u> In this step, the present business process is analyzed and documented. The key deliverable of this step includes the well-defined short-comings of the present processes and the overall business requirements. This step includes the following activities:

- *Understanding the business and the objectives for which it exists;*
- *Documenting the existing business processes; and*
- *Analysis of the documented processes.*

(ii) <u>Proposed Process Documentation:</u> This step is to design the new process requirements for the system. The design is based on the new system requirements and the changes proposed. The activities include the following:

- *Understanding of the business processes necessary to achieve the business objectives;*
- *Designing the new processes; and*
- *Documentation of the new process, preferably using CASE tools.*

(iii) <u>Implementation of New Process:</u> This step is to implement largely the new as well as modified processes at the entity. The critical activities may include the following:

- *Validating the new process;*
- *Implementing the new process; and*
- *Testing the new process.*

(b) Network Access Control can be achieved through following means:

- ***Policy on use of network services**: An enterprise wide policy applicable to internet service requirements aligned with the business need for using the Internet services is the first step. Selection of appropriate services and approval to access them should be part of this policy.*
- ***Enforced path:** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; e.g.. internet access by employees will be routed through a firewall and proxy.*
- ***Segregation of networks:** Based on the sensitive information handling function; say a VPN connection between a branch office and the head-office, this network is to be isolated from the internet usage service.*
- ***Network connection and routing control:** The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility.*
- ***Security of network services:** The techniques of authentication and authorization policy should be implemented across the organization's network.*
- ***Firewall:** Organizations connected to the Internet and Intranet often implements an electronic firewall to insulate their network from intrude. A Firewall is a system that enforces access control between two networks. To accomplish this, all traffic between the external network and the organization's Intranet must pass through the firewall. Only authorized traffic between the organization and the outside can pass through the firewall. The firewall must be immune to penetrate from both outside and inside the organization. In addition to insulating the organization's network from external networks, firewalls can be used to insulate portions of the organization's Intranet from internal access also.*
- ***Encryption**: Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm and the original message called the clear text is converted into cipher text. This is decrypted at the receiving end. The encryption algorithm uses a key. The more bits in the key, the stronger are the encryption algorithms. Two general approaches are used for encryption viz. private key and public key encryption.*
- ***Call Back Devices:** It is based on the principle that the key to network security is to keep the intruder off the Intranet rather than imposing security measure after the criminal has connected to the intranet. The call- back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to*

establish a new connection. This limits access only from authorized terminals or telephone numbers and prevents an intruder masquerading as a legitimate user. This also helps to avoid the call forwarding and man-in-the middle attack.

- *Recording of Transaction Log: An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.*

(c) (i) An enterprise with Business Continuity Management (BCM) uses training as a tool to initiate a culture of BCM in all the stakeholders by:

- *Developing a BCM program more efficiently;*
- *Providing confidence in its stakeholders (especially staff and customers) in its ability to handle business disruptions;*
- *Increasing its resilience over time by ensuring BCM implications are considered in decisions at all levels; and*
- *Minimizing the likelihood and impact of disruptions.*

(ii) Development of a BCM culture is supported by:

- *Leadership from senior personnel in the enterprise;*
- *Assignment of responsibilities;*
- *Awareness raising;*
- *Skills training; and*
- *Exercising plans.*

(d) Auditors might use System Control Audit Review File (SCARF) to collect the following types of information:

- *Application System Errors: SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.*
- *Policy and Procedural Variances: Organizations must adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.*
- *System Exception: SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the*

prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.

- ***Statistical Sample**: Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.*
- ***Snapshots and Extended Records**: Snapshots and extended records can be written into the SCARF file and printed when required.*
- ***Profiling Data**: Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.*
- ***Performance Measurement**: Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.*