ISCA – Case Studies.

1. **A retail company has been in the process converting its manual sales counters into a computerized system with the implementation of a Point of Sales (POS) system for the last 6 months. The company needs to evaluate the software application system for its completeness, correctness and quality.**

   Read the scenario carefully and answer the following:

   a. **State the test plan to be performed to check if the different modules of the application are integrated seamlessly.**
   b. **Identify the testing method to verify that the application is efficient to handle about500 POS counters concurrently.**
   c. **Explain the testing method used to test the consistency between different versions of the same application. [RTP. NOV 2009]**

   Answer:
   When there are multiple modules present in an application, the sequence in which they are to be integrated need to be specified in this integration test plan. In this, the dependencies between the modules play a vital role. If a unit B has to be executed, it may need the data that is fed by unit A and unit X. In this case, the units A and X have to be integrated and then using that data, the unit B has to be tested. This has to be stated to the whole set of units in the program. Given this correctly, the testing activities will lead to the product, slowly building the product, unit by unit and then integrating them. The integration test plan is the overall plan for carrying out the activities in the integration test level, which contains the kinds of interfaces which fall under the scope of testing viz., internal and external interfaces and how the interfaces are triggered is explained.

   (a) To test the behavior of the application system when the maximum number of users and concurrently active and when the database contains the greatest data volume. The creation of a volume test environment requires considerable effort. It is essential that the correct level of complexity exists in terms of the data within the database and the range of transactions and data used by the scripted users, if the tests are to reliably reflect the production environment. Once the test environment is built it must be fully utilized. Volume tests offer much more than simple service delivery measurement. The exercise should seek to answer the following questions:

   - What service level can be guaranteed? How can it be specified and monitored?
   - Are changes in user behavior likely? What impact will such changes have on resource consumption and service delivery?
   - Which transactions/processes is resource hungry in relation to their tasks?
   - What are the resource bottlenecks? Can they be addressed?
   - How much spare capacity is there?
   - The purpose of volume testing is to find weaknesses in the system with respect to its handling of large amount of data during extended time periods.

   (b) Parallel Testing ensures that the processing of new application (new version) is consistent with respect to the processing of previous application version.
   - Conducting redundant processing to ensure that the new version or application performs correctly.
   - Demonstrating consistency and inconsistency between 2 versions of the application.
   - The same input data should be run through 2 versions of same application system.
   - This testing can be done with whole system or part of system (segment).
   - When there is uncertainty regarding correctness of processing of new application where the new and old version are similar.

2. **An auditor while evaluating the reliability of a control implemented in a transaction process, had to estimate the reliability per transaction. A test was undertaken and the result indicated that the control was unreliable. The reliability of the process was 0.15 when the control was in place and was 0.09 when the control was absent. The management had estimated the cost of reprocessing the errors as Rs.1000 per transaction procedure. Evaluate the net benefit of the control procedure if the cost of implementation of the control is Rs.10, 000. [RTP. NOV 2009]**

Answer:

The benefit and reliability of the control is evaluated that when the control procedure for validation is absent the expected loss to the company per transaction is Rs. 100/- and the expected net benefit of implementing the control results in Rs. 400/ - and hence validates its reliability.

Reliability of a control in a transaction process	out Validation Procedure	Validation Procedure	Expected Difference
Cost to reprocess the transaction process	Rs 10,000	Rs 10,000	
Risk of payroll data errors	0.09	0.15	
Expected reprocessing cost (Rs. 10,000 X risk)	Rs.1,000	Rs.500	Rs.500
Cost of validation procedure per transaction	Rs.0	Rs.1000	Rs.1000
Net expected benefit of validation procedure			Rs. 500

3. **ABC university currently provides the ability to register for classes via an enterprise software system within its intranet. However, the university is in the process of modifying its student registration system to allow registrations via the web. Based on the given case, answer the following:**
   (a) As an IS Auditor, suggest the change controls to be implemented to monitor the change.
   (b) Role of an IS auditor in evaluating the logical access controls implemented in the new system.
   (c) As an IS Auditor, list the issues that need to be considered for quality control.
   [RTP. NOV 2009]

Answer:

(a) To properly control information system changes, the university needs formal change management control policies and procedure. These controls should include the following:

- Periodically review all systems for needed changes.
- Require all requests to be submitted in a standardized format.
- Log and review requests from authorized users for changes and additions to systems.
- Assess the impact of requested changes on system reliability objectives, policies and standards.
- Categorize and rank all changes using established priorities.
- Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is as audit trail for all urgent matters.
- Communication all changes to management and keep change requestors informed of the status of their requested changes.
- Require IT management to review, monitor, and approve all changes to hardware, software, and personnel responsibilities.
- Assign specific responsibilities to those involved in the change and monitor their work. Make sure that the specific assignments result in an adequate segregation of duties.
- Control system access rights to avoid unauthorized systems and date access.
- Make sure all changes go through the appropriate steps (development, testing, and implementation).
- Test all changes to hardware, infrastructure, and software extensively in a separate, non production environment before placing it into live production mode.
- Make sure there is a plan for backing out of any changes to mission -critical systems in the event that it does not work or does not operate properly.

- Implement a quality assurance function to ensure that all standards and procedures are followed and to assess if change activities achieve their stated objectives. These findings should be communicated to user departments, information systems management, and top management.
- Update all documentation and procedures when changes are implemented.

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

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

(c) The following are the general questions that the auditor will need to consider for quality control:-

Does system design follow a defined and acceptable standard?

- ⇨ Are completed designs discussed and agreed with the users? (Perhaps with the assistance of prototypes - see Chapter 8);
- ⇨ does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organization's technical standards and policies, and the User Requirements Specification;
- ⇨ Do quality reviews follow a defined and acceptable standard?
- ⇨ are quality reviews are carried out under the direction of a technically competent person who is managerially independent from the design team;
- ⇨ Is auditors/security staff invited to comment on the internal control aspects of system designs and development specifications?
- ⇨ Are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
- ⇨ Are defects uncovered during quality reviews always corrected?
- ⇨ Does the production of development specifications also include the production of relevant acceptance criteria?
- ⇨ Has a Configuration Manager been appointed? Has the configuration management role been adequately defined?
- ⇨ are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?
- ⇨ has sufficient IT (in the form of spreadsheets, databases, and specialist configuration management support tools) been provided to assist with the configuration management task?
- ⇨ Are effective procedures in place for recording, analyzing and reporting failures uncovered during testing?
- ⇨ Are effective change management procedures are in place to control changes to configuration items?
- ⇨ Has a System Installation Plan been developed and quality reviewed?
- ⇨ Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery? (To avoid "skills stagnation", the delivery of training will need to be carefully scheduled);
- ⇨ Has an Acceptance Testing Plan been drawn up? Is it to an acceptable standard? Does it cover all aspects of the User Requirements Specification?

- ⇨ Does the Acceptance Test Plan clearly allocate roles and responsibilities for undertaking and reviewing the results of acceptance testing?
- ⇨ Has the Acceptance Test Plan been discussed with, and signed off by, the prospective System Owner?
- ⇨ Is the system development environment is regularly backed up with copies of backed up configuration items held securely at a remote location?
- ⇨ Has the development environment been recovered from backup media?
- ⇨ Are contingency plans commensurate (in terms of time to implement) with the criticality of the project?
- ⇨ do regular Project Board meetings take place to review project progress against budget and deadline?
- ⇨ Is the Business Case regularly updated to ensure that the project remains viable?

4. A company is developing several types of biscuits, having its branches all over the country. The owner of the company wishes to centralize and consolidate the information flowing from its branches in a uniform manner across various levels of the organization. The technical advisor of the company recommended that the company should go for the implementation of the ERP Package. Why the company should undertake ERP?

(a) What is Business Process Reengineering? Explain in brief.

(b) Explain the criterion for evaluation of various ERP Packages in brief. [RTP. NOV 2009]

Answer:

(a) Business Process Reengineering(BPR): The most accepted and formal definition for BPR, given by Hammer and Champhy is reproduced here: " BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement, in critical, contemporary measures of performance such as cost, quality, service and speed," This has a few important key words, which need clear understanding. Here, dramatic achievement means to achieve 80% or 90% reduction (in say, delivery time, and work in progress or rejection rate) and not just 5%,

This is possible only by making major improvements and breakthroughs, and not small incremental changes (like those in Total Quality Management (TQM) or suggestion schemes).

Radical redesign means BPR is reinventing and not enhancing or improving. In a nutshell, a "cleansiate approach" of BPR says that "Whatever you were doing in the past is all wrong", do not get biased by it or reassemble the new system to redesign it afresh. Fundamental rethinking means asking the question "why do you do what you do", thereby eliminating business process altogether if it does not add any value to the customer. There is no point in simplifying or automating a business process which does not add any value to the customer. A class example is that of asking for an invoice from the supplier for payment when the company has already received and accepted a particular quantity of material physically and at an agreed price. Receiving, processing, and filing of invoices add no value to the customer and makes only the supplier unhappy for delayed payments. Thus, BPR aims at major transformation of the business processes to achieve dramatic improvement. Here, the business objectives of the Enterprise (e.g., profits, customer – satisfaction through optimal cost, quality, deliveries etc.) are achieved by "transformation" of the business processes which may, or may not, require the use of Information Technology (IT).

(b) **Criteria for the evaluation of various ERP packages**: Evaluation of ERP packages are done based on the following criteria:-

Flexibility: It should enable organizations to respond quickly by leveraging changes to their advantage, letting them concentrate on strategically expanding and to address new products and markets.

Comprehensive*:* It should be applicable across all sizes, functions and industries. It should have in-depth features in accounting and controlling, production and materials management, quality management and plant maintenance, sales and distribution, human resources management and plant maintenance, sales and distribution, human resources management, and project management. It should also have information and early warning systems for each function and

enterprise -wide business intelligence system for informed decision making at all levels. It should be open and modular.

It should embrace an architecture that supports components or modules, which can be used individually, expandable in stages to meet the specific requirements of the business, including industry specific functionality. It should be technology Independent and mesh smoothly with in-house/third-party applications, solutions and services including the Web.

***Integrated*:** It should overcome the limitations of traditional hierarchical and function oriented structures. Functions like sales and materials planning, production planning, warehouse management, financial accounting, and human resources management should be integrated into a workflow of business events and processes across departments and functional areas, enabling knowledge workers to receive the right information and documents at the right time at their desktops across organizational and geographical boundaries.

Beyond the company : It should support and enable inter-enterprise business processes with customers, suppliers, banks, government and business partners and create complete logistical chains covering the entire route from supply to delivery, across multiple geographies, currencies and country specific business rules.

Best business practices: The software should enable integration of all business operation in an overall system for planning, controlling and monitoring and offer a choice of multiple ready-made business processes including best business practices that reflect the experiences, suggestions and requirements of leading companies across industries. In other words, it should intrinsically have a rich wealth of business and organizational knowledge base.

***New technologies*:** It should incorporate cutting-edge and future-proof technologies such as object orientation into product development and ensure inter -operability with the Internet and other emerging technologies.

It should be Y2K and Euro compliant, group up.

Other factors to be considered are:

- Global presence of package.
- Local presence.
- Market Targeted by the package.
- Price of the package.
- Obsolescence of package.
- Ease of implementation of package.
- Cost of implementation.
- Post-implementation support availability.

5. ABC Company is implementing The Health Insurance Portability and Accountability Act (HIPPA). There is a security rule issued under the Act which lays out three types of security safeguards required for compliance. What are those conditions under these safeguards for which the company should look after? [RTP. NOV 2009]

Answer:

The Security Rule: The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for "small plans". The Security lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. The standards and specifications are as follows:

(i) **Administrative Safeguards -** policies and procedures designed to clearly show how the entity will comply with the act

- ⇨ Covered entities (entities that must comply with HIPAA requirement s) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
- ⇨ The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
- ⇨ Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI). Access to PHI in all forms must be restricted to only those employees who have a need for it to complete their job function.
- ⇨ The procedures must address access authorization, establishment, modification, and termination.
- ⇨ Entities must show that an appropriate ongoing training program regarding the handling PHI is provided to employees performing health plan administrative functions.
- ⇨ Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
- ⇨ A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
- ⇨ Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
- ⇨ Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

(ii) **Physical Safeguards** - controlling physical access to protect against inappropriate access to protected data

- ⇨ Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
- ⇨ Access to equipment containing health information should be carefully controlled and monitored.
- ⇨ Access to hardware and software must be limited to properly authorized individuals.
- ⇨ Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- ⇨ Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
- ⇨ If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

(iii) **Technical Safeguards -** controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

- ⇨ Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
- ⇨ Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner. Data corroboration, including the use of

check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.

- ⇨ Covered entities must also authenticate entities it communicates with. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone call-back, and token systems.
- ⇨ Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
- ⇨ In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
- ⇨ Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a Minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non - health purposes.)

6. An organization is committed to implement the information security policy through established goals and principles. The major problem, organization is facing through its employees. There is neither any proper allocation of duties/ responsibilities between employees nor a proper reporting hierarchy. Suggest a proper security organization structure and responsibility allocation, to come out of these problems. [RTP. NOV 2009]

Answer:
Security Organization Structure: The security responsibility and the line of reporting in the organization should be defined in the policy as stated below:

- ⇨ **Information Security Forum (ISF):** This forum is chaired by the GSO and includes senior representatives from each of the divisions within the Group, together with the AGSO. The AGSO provides the reporting conduit from the ISMG. It is the role of this forum to ensure that there is clear direction and visible management support of security initiatives within the organization.
- ⇨ **Information Security Management Group (ISMG):** This cross functional group is chaired by the AGSO and comprises of a Divisional System Security Officer (DSSO) from each of the divisions within the Group, together with the IT Security Officer (ITSO), and the Personnel and Facilities Management Security Officers. Its role is to co-ordinate the implementation and management of information security controls across all of the divisions and sites.
- ⇨ **Group Security Officer (GSO):** The GSO will have overall responsibility for security within the Group. This includes the security of all information assets, the network accreditation scheme and for non-IT security including physical and personnel matters.
- ⇨ **Assistant Group Security Officer (AGSO):** The AGSO reports to the GSO and the Information Security Forum and is responsible for the co-ordination of information security implementation and management across the Group. The AGSO chairs the ISMG.
- ⇨ **IT Management:** IT Management has overall responsibility for security of the IT infrastructure. This is discharged mainly through Installation Security Officers (ISOs) and the IT Security Officer (ITSO) who will report directly to the IS Service Manager.
- ⇨ **IT Security Officer (ITSO)**: The IT Security Officer reports to the ISMG on IT security matters. The ITSO is responsible for managing IT security programs and IT security incidents. The ITSO will chair regular meetings of the ISO's
- ⇨ **Installation Security Officer (ISO):** An ISO will be appointed for each IT environment (including Network and Desktop) from the IT Team Leaders. ISOs will be responsible for all security matters related to their system/installation and/or network and will meet regularly with the IT Security Officer.
- ⇨ **Personnel Security Officer (PSO):** The Personnel Security Officer (PSO) will report directly to Personnel Management and the ISMG on all security matters relating to personnel. The role involves ensuring the controls set out are implemented, adhered to and reviewed as necessary.
- ⇨ **Facilities Management Security Officer (FMSO):** The Facilities Management Security Officer (FMSO) will report directly to Facilities Management on all security matters relating to personnel. The role involves ensuring the controls are implemented, adhered to and reviewed as necessary.

- ⇨ **Divisional System Security Officer (DSSO):** A System Security Officer (SSO) from each division will be appointed as a DSSO. The DSSO carries the same responsibilities as a SSO and in addition is responsible for representing the SSOs in their division at the ISMG and for communicating requirements and issues to/from this group.
- ⇨ **System Security Officer (SSO):** A senior user will be appointed to fulfill the role of System Security Officer (SSO) for each major application system or group of systems. SSO responsibilities focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.
- ⇨ **System Owners**: System Owners carry the overall responsibility for the information security of their own systems. Much of the day to day operational aspects of live systems may be delegated across a range of user defined roles and technical roles including their systems accreditation process. System Owners are responsible for allocation of protective markings to their systems and data according to the Information Classification policy, and all staff for treating protectively marked material accordingly.

- ⇨ **Line Managers:** All Line Managers with any responsibility for live or developing IT systems must take appropriate steps to ensure compliance with the aims and objectives of this policy. As part of this process they will ensure that all required security measures are understood and in force.
- ⇨ **Users**: All users of live IT systems are required to comply with the security procedures for their system and any applicable general IT security guidance.

A sample structure is given below:

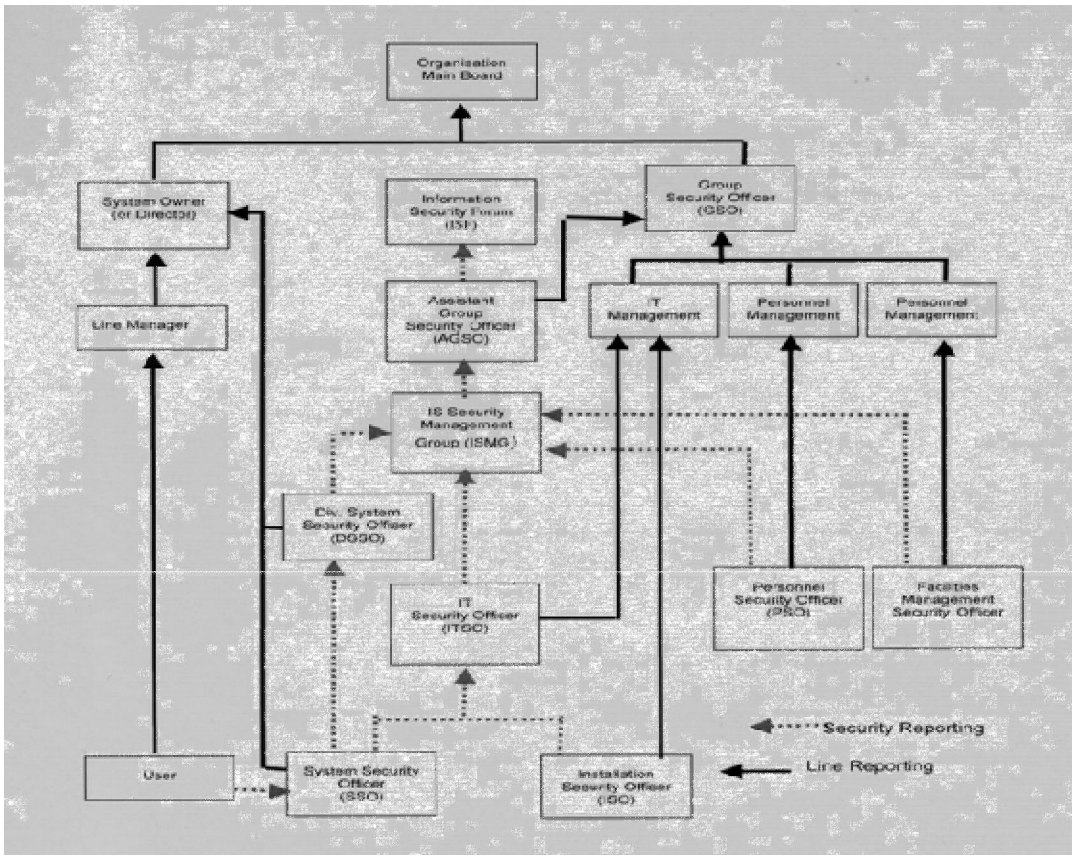


Fig.: The Information Security Organization Structure

Responsibility allocation: The responsibilities for the management of Information Security should be set out in this policy.

- ⇨ An owner would be appointed for each information asset.

- ⇨ All staff should be aware of the need for Information Security and should be aware of their responsibilities.
- ⇨ Been completed successfully and the System Owner is satisfied.
- ⇨ All new network communications links must be approved.
- ⇨ A contact list of organizations that may be required in the event of a security incident to be maintained.
- ⇨ Risk assessments for all third party access to the information assets and the IT Network must be carried out.
- ⇨ Access by third parties to all material related to the IT Network and infrastructure must be strictly limited and controlled. There should be a Conditions of Connection agreement in place for all third party connections.
- ⇨ All outsourcing contracts must detail All major changes to software and hardware including major updates and new versions must be approved. It is not permissible to make the changes to a live system until tests have security responsibilities.

7. an Information Systems Audit Report contains various components: Cover and title page, Table of contents, Summary/Executive summary, and Appendices. But after submission, the principal auditor raised the query that the report is not correct as it missed various important components. Explain the missing components in brief. [RTP. NOV 2009]

Answer:
The missing components of the said IS Audit report are given as follows:

(i) **Introduction:** Since readers will read the summary, the introduction should not repeat details. It should include the following elements:

- **Context:** This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.
- **Purpose:** This sub-section is a short description of what functions and special programs were audited and the clients' authorities.
- **Scope:** The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.
- **Methodology:** This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.

(ii) **Findings:** Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives and clients' expectations. If the auditor is using any standard grading standard like InfoSecGrade or others, the arrived value should also be stated.

(iii) **Opinion**: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.

8. as a member of the system development team, explain the process of decomposition of an organization into various functional blocks to comprehend the information processing system with the help of an example. [RTP. MAY 2010]

Answer:
A **system** functions with a collection of elements organized as a group of interdependent functioning units or components, linked together according to a plan, to achieve a specific objective. These elements surround the system and often interact with it. The feature that defines and delineates a system forms its boundary. The system is inside the **boundary**; the environment is outside the boundary.

A system and its environment can be described with **subsystems** that are a part of a larger system. Each system is composed of subsystems, which in turn are made up of other subsystems, each sub-system

being delineated by its boundaries. The interconnections and interactions between the subsystems are termed **interfaces.** Interfaces occur at the boundary and take the form of inputs and outputs.

A complex system is difficult to comprehend when considered as a whole. Therefore the system is decomposed or factored into subsystems. The boundaries and interfaces are defined, so that the sum of the subsystems constitutes the entire system. This process of decomposition is continued within subsystems divided into smaller subsystems until the smallest subsystems are of manageable size.

Doing business is also a system with its components being marketing, manufacturing, sales, research, shipping, accounting and personnel. All these components work together with a common focus to create a profit that benefits the organization.

All systems have some common characteristics that justify the need for decomposition. These are given as follows:

- ⇨ All systems work for predetermined objectives and the system is designed and developed accordingly.
- ⇨ In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
- ⇨ If one subsystem or component of a system fails, in most cases the whole system does not work. However, it depends on how the subsystems are interrelated.
- ⇨ The way a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system
- ⇨ The work done by individual subsystems is integrated to achieve the central goal of the system. The goal of individual subsystem is of lower priority than the goal of the entire system.

An example of the decomposition is the factoring of an information processing system into subsystems. One approach to decomposition might proceed as follows:

(i) Information system divided into subsystem such as:

a. Sales and order entry
b. Inventory
c. Production
d. Personnel and payroll
e. Purchasing
f. Accounting and control
g. Planning
h. Environmental intelligence

(ii) Each subsystem is divided further into subsystems. For example, the personnel and payroll subsystem might be divided into the following smaller subsystems:

a. Creation and update of personnel pay-roll records
b. Personnel reports
c. Payroll data entry and validation
d. Hourly payroll processing
e. Salaried payroll processing
f. Payroll reports for management
g. Payroll reports for government

(iii) If the task is to design and program a new system, the subsystems (major applications) defined in might be further subdivided into smaller subsystems or modules. For example, the hourly payroll processing subsystem might be factored into modules for the calculation of deductions and net pay, payroll register and audit controls preparation, cheque printing, and register and controls output.

9. An organization is in the stage of systems development to implement an enterprise wide information system, where the following conditions exist:

- **End users are not aware of the information needs.**
- **The new system is mission critical and there is a hasty need.**
- **The business risks associated in implementing the wrong system are high. Read the above case carefully and answer the following with proper justification/s:**

(a) Identify the system development approach and the steps to be followed in the above stated conditions.
(b) State the reasons for choosing the particular approach for system development.
(c) Identify the risks, when end-users are involved in the system development process.
[RTP. MAY 2010]

Answer:

(a) Evaluation and validation of the software package to be acquired needs to meet the following features to ascertain before purchasing:

- ⇨ What is the package designed to do?
- ⇨ How is the package organized and operable to the present value chain?
- ⇨ Can the package operate on our hardware configuration?
- ⇨ Can the program provide the needed reports?
- ⇨ Does the program have adequate capacity in terms of the number of transactions it can process, the number and length of fields per record it can process, the total file size permitted and so on?
- ⇨ How many processing runs on the computer are required to complete each data processing job?
- ⇨ How long does the program take to process?
- ⇨ Will the package require modifications and how often?
- ⇨ What are the overall costs on modifications and maintenance?
- ⇨ Is comprehensive documentation available?
- ⇨ What are the package constraints?
- ⇨ Where the package is currently utilized?
- ⇨ What input/output techniques are utilized?
- ⇨ What are the required input/output formats?
- ⇨ What controls are included?
- ⇨ What kind of user training is provided?

(b) To evaluate and validate the Support Service to be acquired from a vendor, major features to be ascertained are:

- ➢ *Performance*: What has been the vendor's past performance in terms of his past promises?
- ➢ *System development*: Are system analysis and programming consultants available? What are their qualities and cost?
- ➢ *Maintenance*: Is equipment maintenance provided? What is the quality and cost?
- ➢ *Conversion*: What systems development, programming and hardware installation service will they provide during the conversion period?
- ➢ *Training*: Is the necessary training of personnel provided? What is its quality and cost?
- ➢ *Back-up*: Are several similar computer facilities available for emergency back - up purposes?
- ➢ *Proximity*: Does the vendor have a local office? Are sales, systems development, programming, and hardware maintenance services provided from the office?
- ➢ *Hardware*: Do they have a wide selection of compatible hardware?
- ➢ *Software*: Do they have a wide variety of useful systems software application programs?

(c) A Software License Agreement (SLA) is a license that grants permission to do things with computer software. The license is to authorize activities which are prohibited by default by copyright law, patent law, trademark law and any other intellectual property right. The coverage of the license includes:

- ⇨ The SLA is to encourage disclosure of the intellectual property.
- ⇨ A method to allow the licensed user to use the product but still be restricted so as to prevent certain decompiling rights the user might otherwise have as a result of the default intellectual property rights.
- ⇨ It identifies the specific usage rights that are granted to the licensee, while also stating the license limitations.
- ⇨ A software license is to specify permission to allow a certain number of concurrent users of the software.
- ⇨ Administrator and user license copies are to be clearly documented.

- ⇨ A software vendor may offer software license proprietary software sold from a single vendor or a joint agreement with one or more vendors.
- ⇨ The SLA is to cover the distribution terms under the EULA (End-User License Agreement) is a legal contract between the manufacturer and/or the author and the end user of an application.
- ⇨ EULA terms are to be followed in a SLA including free software and open source software.
- ⇨ The SLA should also state the default penalties for violations of intellectual property laws in and if so allowed by the geographic region of the licensor, as well as any terms contractually agreed-upon damages listed in the software license.

10. the table, given below contains the exposures or vulnerabilities. As an IS Auditor, identify the control type and the control technique to be implemented to mitigate the risk.

S. No.	Exposure
(a)	**Records or files assigned to a particular user being modified by another user.**
(b)	**Anybody can enter the server room.**
(c)	**To change the contents of the web pages published on a company's server.**
(d)	**Failure of hard disks in the database storage system due to spikes in the electrical supply and heating.**
(e)	**The system development projects/tasks consume excessive resources and unauthorized system changes are recorded.**

[RTP. MAY 2010]

Answer:

Exposure: Records or files assigned to a particular user being modified by another user.

Access Control Type: Logical access control.
Control Techniques:
Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. They restrict users to authorized transactions and functions.
An access control mechanism associates with identified and authorized users to the resources they are allowable to access and action privileges. The mechanism processes the users request for resources in the following sequence:
*First, the users have to identify themselves, thereby indicating their intent to request the usage of system resources.
*Secondly, the users must authenticate themselves and the mechanism must authenticate itself.
*Third, the users request for specific resources, their need for those resources and their areas of usage of these resources.

The mechanism accesses previously stored information about users, the resources they can access, and the action privileges they have with respect to these resources; it then permits or denies the request. Users identify themselves to access control mechanism by providing authentication information such as:

Remembered information	Name, Account number, passwords
Objects Possessed by the user	Badge, plastic card, key
Personal characteristics	Finger print, voice print, signature
Dialog	Through/around computer

The authorization module then functions in terms of a matrix where rows represent the users and columns represent the resources and the element represents the user's privilege on the resources:

This mechanism operates via a column in the Authorization matrix:

Resource User	File A	Editor	File B	Program
User P	Read	Enter		
User Q	Statistical Read only	Enter		Enter
User R		Enter	Append only	
User S		Enter		Read Resource Code only

Each user process has a pointer to the access control list (matrix) for a resource. Thus the capabilities for a resource can be controlled as they are stored in one place. It is enough to examine the access control list just to know who has access over the resource and similarly to revoke access to a resource, a user's entry in the access control list simply needs to be deleted.

(b) Exposure: Anybody can enter the server room.

Access Control Type*:* Physical Access Control.

Control Techniques: Physical access controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. These controls should be designed in such a way that it allows access only to authorized persons. The authorization given by the management may be explicit, as in a door lock for which management has authorized a person to have a key; or implicit, like a job description which confirms the need to access confidential reports and documents or a server room.

Some of the more common access control techniques are:
(i) Locks on Doors:

- ⇨ *Cipher locks (Combination Door Locks)* - The cipher lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.
- ⇨ *Bolting Door Locks – A special metal key is used to gain entry when the lock is a bolting* door lock. To avoid illegal entry the keys should be not be duplicated.
- ⇨ *Electronic Door Locks* – A magnetic or embedded chip-based plastics card key or token may be entered into a sensor reader to gain access in these systems. The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism.
- ⇨ *Biometric Door Locks* **–** These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

(ii) Physical identification medium

- ⇨ *Personal Identification numbers (PIN)* **–** A secret number will be assigned to the individual, which serves to verify the authenticity of the individual by inserting a card in some device and then enter their PIN via a PIN keypad for authentication.

- ⇨ *Plastic Cards*- These cards are used for identification purposes. Controls over card seek to ensure that customers safeguard their card so it does not fall into unauthorized hands.

(iii) Logging on utilities

- ⇨ *Manual Logging*- All visitors should be prompted to sign a visitor's log indicating their name, company represented their purpose of visit, and person to see.

- ⇨ *Electronic Logging* – This feature is a combination of electronic and biometric security systems. The users logging in can be monitored and the unsuccessful attempts being highlighted.

(c) Exposure: To change the contents of the web pages published on a company's server.

Access Control Type: Network Access Control.

Control Techniques: Monitoring network to detect week points and multiple communication paths between networks components are done by using preventive maintenance controls. These controls include data encryption, routing verification and message acknowledgement procedures. The implementation of these controls is performed by firewalls and intrusion detection systems (IDSs).

(i) Firewalls: A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs).

Here an Application-level firewall will perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. It examines each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers.

(ii) Intrusion Detection Systems: This is placed between the firewall and the system being secured, and provides an extra layer of protection to that system. It monitors access from the internet to the sensitive data ports of the secured system and can determine whether the firewall has perhaps been compromised, or whether an unknown mechanism has been used to bypass the security mechanisms of the firewall to access the network being protected.

The types of Intrusion Detection systems are:

⇨ *Network based systems.* Are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries.

⇨ *Host based systems.* These types of systems actually run on the system being monitored. These examine the system to determine whether the activity on the system is acceptable.

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

(d) **Exposure:** Failure of hard disks in the database storage system due to spikes in the electrical supply and heating.
Access Control Type: Environmental Access Control.

Control Techniques: The environmental security measures are taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Assessing the environmental protection involves evaluating if the controls have been implemented and are commensurate with the risks of physical damage or access. The control techniques required to mitigate the identified exposure are:

(i) *Electrical Surge Protectors:* The risk of damage due to power spikes are reduced by using electrical surge protectors.

- ⇨ The incoming current is measured and monitored by the voltage regulator, ensures consistent current.
- ⇨ These are typically built into the Uninterruptible Power Supply (UPS) system.

(ii) Uninterruptible Power Supply (UPS) / Generator: A UPS system consists of a battery or gasoline powered generator that interfaces between the electrical power entering the facility and the electrical power entering the computer.

⇨ It cleanses the power to ensure wattage into the computer is consistent.

⇨ In case of a power failure, the UPS provides the back up by providing electrical power from the generator to the computer for a certain span of time (a few minutes up to few hours) to permit an orderly computer shutdown.

*(iii) Emergency Power-Off Switch***:** The need for immediate power shut down arises during situations like a computer room fire or an emergency evacuation, a two emergency power-off switch one at computer room and other near but outside the computer room and easily accessible, yet secured from unauthorized access is mandatory.

(iv) Humidity/Temperature Control: Sensors/Alarms in the information processing facility to monitor on regular intervals and determine if temperature and humidity are adequate.

(e) Exposure: The system development projects/tasks consume excessive resources and unauthorized system changes are recorded.

Access Control Type: Change management controls.

Control Techniques: To properly control information system changes, companies need formal change management control policies and procedure. These controls should include the following:

⇨ Periodically review all systems for needed changes and requirements are to be submitted in a standardized format.

⇨ Log and review requests from authorized users for changes and additions to systems.

⇨ Assess the impact of requested changes on system reliability objectives, policies and standards.

⇨ Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is as audit trail for all urgent matters.

⇨ Communication all changes to management and keep change requestors informed of the status of their requested changes.

⇨ Require IT management to review, monitor, and approve all changes to hardware, software, and personnel responsibilities.

⇨ Assign specific responsibilities to those involved in the change and monitor their work. Make sure that the specific assignments result in an adequate segregation of duties.

⇨ Make sure all changes go through the appropriate steps (development, testing, and implementation).

⇨ Test all changes to hardware, infrastructure, and software extensively in a separate, non production environment before placing it into live production mode.

⇨ Make sure there is a plan for backing out of any changes to mission-critical systems in the event that it does not work or does not operate properly.

⇨ Implement a quality assurance function to ensure that all standards and procedures are followed and to assess if change activities achieve their stated objectives. These findings should be communicated to user departments, information systems management, and top management.

⇨ Update all documentation and procedures when changes are implemented.

11. As a member of the system implementation and quality control team, prepare a quality control review checklist from an IS Auditor's perspective. [RTP. MAY 2010]

Answer:
For an IS Auditor, to carry out detailed reviews of system logical design and quality control the general questions to be answered are stated below:

(a) Does system design follow a defined and acceptable standard?

(b) Are completed designs discussed and agreed with the users? (perhaps with the assistance of prototypes);

(c) Does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organization's technical standards and policies, and the User Requirements Specification;

(d) Do quality reviews follow a defined and acceptable standard?

(e) are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;

(f) Are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?

(g) Are defects uncovered during quality reviews always corrected?

(h) Does the production of development specifications also include the production of relevant acceptance criteria?

(i) Has a Configuration Manager been appointed? Has the configuration management role been adequately defined?

(j) Are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?

(k) Has sufficient IT (in the form of spreadsheets, databases, and specialist configuration management support tools) been provided to assist with the configuration management task?

(l) Are effective procedures in place for recording, analysing and reporting failures uncovered during testing?

(m) Are effective change management procedures are in place to control changes to configuration items?

(n) Has a System Installation Plan been developed and quality reviewed?

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

(p) Is the system development environment is regularly backed up with copies of backed up configuration items held securely at a remote location?

(q) Are contingency plans commensurate (in terms of time to implement) with the criticality of the project?

(r) Do regular Project Board meetings take place to review project progress against budget and deadline?
Is the Business Case regularly updated to ensure that the project remains viable?

12. A Telecom organization produces information on a real-time and online basis which requires real-time auditing on the quality of the data and auditor's assurance testing. Identify the audit tool that tags the online transactions and collects audit evidence in a dummy entity. [RTP. MAY 2010]

Answer:
A Telecom organization produces information on a real-time, online basis which requires real-time recordings and real-time auditing to ensure continuous assurance about the quality of the data. Continuous auditing enables auditors to significantly reduce and perhaps eliminate the time between occurrence of the client's events and the auditor's assurance services thereon.

Errors in a computerized system are generated at high speeds and the cost to correct and rerun programs are high. If these errors can be detected and corrected at the point or closest to the point of their occurrence, the impact thereof would be the least. The continuous auditing technique to collect audit evidence by tagging transactions is called the **Integrated Test Facility (ITF).**
The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included along with the normal production data and given as input to the application system. The two methods to audit are:

(i) *Methods of Entering Test Data*:

- ⇨ The transactions to be tested are to be tagged.
- ⇨ The application system is programmed to recognize the tagged transactions and invoke two updates namely the application system master file record and the ITF dummy entity.
- ⇨ The live transactions can also be tagged as ITF transactions, provide ease of use and testing with transactions representative of normal system processing.
- ⇨ Test transactions are entered along with the production input into the application system.
- ⇨ The test data is likely to achieve a complete coverage of the execution paths in the application system to be tested than a selected production data.

(ii) *Methods of Removing the Effects of ITF Transactions:*

- ⇨ The presence of ITF transactions within an application system affects the output results obtained.
- ⇨ The application system is programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users.
- ⇨ Another method is removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions.
- ⇨ Otherwise, to submit trivial entries so that the effects of the ITF transactions on the output are minimal.

13. As an internal auditor of an enterprise, which has acquired and implemented an ERP system in its headquarters and five regional branch offices, how will you perform the testing of general and automated controls on the following issues:

(a) The flow of data and information between the headquarters and the five branch offices,
(b) The concurrent usage of 1000 employees on an average across the offices at anytime, and

(c) The data processing and report generation is in tune with the management objectives. [RTP. MAY 2010]

Answer:
To test the flow of data and information between the headquarters and the five branch offices were an enterprise-wide application is implemented to process the business cycle, the testing method used is called the **Inter System Testing**.

This test method ensures that the data flow and interconnection between the application systems function correctly.

The objectives of this test are:

- ⇨ Proper parameters and data are correctly passed between the applications
- ⇨ Documentation for involved system is correct and accurate.
- ⇨ Proper timing and coordination of functions exists between the application systems.

The method of testing involves:

- ⇨ Operations of multiple systems are tested.
- ⇨ Multiple systems are run from one another to check that they are acceptable and processed properly.
- ⇨ The testing also ensures synchronization when there is a change in the parameters of the application system.
- ⇨ The parameters, which are erroneous and the risk associated to such parameters decide the extent of testing and type of testing.
- ⇨ Intersystem parameters are checked and verified after the change or when a new application is placed in the production.

(b) To test if concurrent usage of 1000 employees on an average across the offices at anytime is feasible on the implemented ERP system, the **Volume testing method** is followed.
The test method checks the behaviour of the enterprise-wide system when the maximum number of users are logged concurrently and when the database contains the greatest data volume.

This test method involves:

- ⇨ Creation of a large volume test environment.
- ⇨ It tests the level of complexity in terms of the data within the database and the range of transactions and data used by the users.
- ⇨ The test tries to reliably reflect the production environment.
- ⇨ Volume tests offer much more than simple service delivery measurement. The test answers the following questions:
- ⇨ What service level can be guaranteed? How can it be specified and monitored?
- ⇨ Are changes in user behaviour likely? What impact will such changes have on resource consumption and service delivery?
- ⇨ Which transactions/processes is resource hungry in relation to their tasks?
- ⇨ What are the resource bottlenecks? Can they be addressed?
- ⇨ How much spare capacity is there?
- ⇨ The volume testing brings out the weaknesses in the system with respect to its handling of large amount of data during extended time periods

(c) **Control testing,** ensures if the data processed and report generation done by the implemented ERP is in tune with the management objectives. It is a management tool to ensure that processing is performed in accordance to management desire s or intent. This testing method is used in parallel with the other system tests.

The testing ensures that:

- ⇨ the data is accurate and complete.
- ⇨ the transactions are authorized.
- ⇨ there is adequate maintenance of audit trail information.
- ⇨ the data processing facilities are efficient, effective and economical.
- ⇨ the processing tasks meet the needs of the user. In performing the control testing:
- ⇨ the system risks are identified.
- ⇨ the testers determine or anticipate what can go wrong in the application system with a negative approach.
- ⇨ the risk matrix is developed to identify the risks, controls; segments within application system in which control resides.

14. An enterprise is in the process of leveraging Information and Communication Technology (ICT) for its business value chain process. As a member of ICT implementation team, prepare the risk assessment lists for the following issues:
(a) Insurance Coverage, and
(b) Enterprise-wide Application Software Security. [RTP. MAY 2010]

Answer:
Risk assessment is a critical step in disaster and business continuity planning. It is the process of identifying threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status within the minimum time in case of a disaster. It is a useful technique to assess the risks involved in the event of unavailability of information, to prioritize applications, identify exposures and develop recovery scenarios.

(a) *Insurance coverage list:* The information system insurance policy should be a multi- peril policy, designed to provide various types of coverage. Depending on the individual organization and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:

- ⇨ Hardware and facilities: The equipment should be covered adequately. Provision should be made for the replacement of all equipment with a new one by the same vendor.
- ⇨ Software reconstruction: In addition to the cost of media, programming costs for recreating the software should also be covered.
- ⇨ Extra expenses: The cost incurred for continuing the operations till the original facility is restored should also be covered.
- ⇨ Business interruption: This applies mainly to centers performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.
- ⇨ Valuable paper and records: The actual cost of valuable papers and records stored in the insured premises should be covered.
- ⇨ Errors and omissions: This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmers and other information system personnel.
- ⇨ Fidelity coverage: This coverage is for acts of employees, more so in the case of financial institutions which use their own computers for providing services to clients.

⇨ Media transportation**:** The potential loss or damage to media while being transported to off-site storage/premises should be covered.

(b) All software applications or the enterprise-wide applications are to be inventoried and the critical points of access are identified. Each of the critical application is reviewed to assess its impact on the organization, in case of a disaster. **Appropriate recovery plans** are developed to address the following issues.

(i) *Identifying critical applications*: Amongst the applications currently being processed the critical applications are identified. They are analyzed to determine specific jobs/functions which are critical for smooth functioning of a value chain.

(ii) *Assessing their impact on the organization*: Business continuity planning not only concentrate on business disruption but also take into account organizational functions which may be affected. The areas to be considered are:

⇨ Legal liabilities,

⇨ Interruptions of customer services,

⇨ Losses on assets, and

⇨ Likelihood of fraud and recovery procedures.

(iii) *Determining recovery time-frame*: Critical recovery time period is the time within which business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature o f operations. It is essential to involve the end users in the identification of critical functions and critical recovery time period.

The other risks to be assessed are:

⇨ Are updated and acceptable standards, policies and guidelines about application software security distributed to concerned employees and are they adequate?

⇨ Are computer security requirements made explicit during new system development and maintenance work?

⇨ Do functional users and auditors participate in system development and maintenance?

⇨ Is there any standard system development and maintenance methodology and is it followed?

⇨ Are software packages purchased and used?

⇨ Do end-users develop and maintain systems using fourth generation languages?

⇨ Have the application software aspects been audited?

15. A backup plan is to be prepared for XYZ company in order to specify the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making a backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recover various systems, and a time frame for the recovery of each system. But the most difficult part in preparing the backup plan is to ensure that all the critical resources are backed up. List the resources that are to be considered in a backup plan. [RTP. MAY 2010]

Answer:
The resources to be considered in the **backup plan** are:

- ⇨ **Personnel:** Training and rotation of duties among information system staff to enable them to replace others when required. Arrangements with another company for provision of staff on need.
- ⇨ **Hardware:** Arrangements with another company for provision of hardware.
- ⇨ **Facilities:** Arrangements with another company for provision of facilities.
- ⇨ **Documentation:** Inventory of documentation stored securely on-site and off-site.
- ⇨ **Supplies:** Inventory of critical supplies stored securely on-site and off-site with a list of vendors who provide all supplies.
- ⇨ **Data / information:** Inventory of files stored securely on site and off site.
- ⇨ **Applications software:** Inventory of application software stored on site and off site.
- ⇨ **System software:** Inventory of system software stored securely on site and off site.

16. ABC Limited has migrated from traditional systems to new real-time integrated ERP systems. The technical advisor of the company advised the owner that the company should take necessary steps to analyze several types of risks. Explain those risks in brief. [RTP. MAY 2010]

Answer:
Organizations face several new business risks when they migrate to real-time, integrated ERP systems. Those risks include:

- ⇨ **Single point of failure:** Since all the organization's data and transaction processing is within one application system and transaction processing is within one application system.
- ⇨ **Structural changes:** Significant personnel and organizational structures changes associates with reengineering or redesigning business processes.
- ⇨ **Job role changes:** Transition of traditional user's roles to empowered-based roles with much greater access to enterprise information in real time and the point of control shifting from the back-end financial processes to the front-end point of creation.
- ☞ **Online, real-time:** An online, real-time system environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring of re-entry of information (e.g., if field personnel are unable to transmit orders from handheld terminals, customer service staff may need the skills to enter orders into the ERP system correctly so the production and distribution operations will not be adversely impacted).
- ☞ **Change management:** It is challenging to embrace a tightly integrated environment when different business processes have existed among business units for so long. The level of user acceptance of the system has a significant influence on its success. Users must understand that their actions or inaction have a direct impact upon other users and, therefore, must learn to be more diligent and efficient in the performance of their day-to-day duties. Considerable training is therefore required for what is typically a large number of users.
- ☞ **Distributed computing experience:** Inexperience with implementing and managing distributed computing technology may pose significant challenges.
- ☞ **Broad system access:** Increased remote access by users and outsiders and high integration among application functions allow increased access to application and data.

- **Dependency on external assistance:** Organization accustomed to in-house legacy systems may find they have to rely on external help. Unless such external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to greater risk.

- **Program interfaces and data conversions:** Extensive interfaces and data conversions from legacy systems and other commercial software are often necessary. The exposures of data integrity, security and capacity requirements for ERP are therefore often much higher.

- **Audit expertise:** Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know only a relatively small fraction of the entire ERP's functionality in a particular core module, e.g. FI auditors, who are required to audit the entire organization's business processes, have to maintain a good grasp of all the core modules to function effectively.

17. (a) An Information System Audit Report includes various sect ions: Title Page, Table of Contents, Summary, Introduction, Findings and Appendices. Explain various elements, included in the 'Introduction' section.

(b) It is clear from various instances that there are not only many direct and indirect benefits from the use of information systems, but also many direct and indirect risks related to the use of information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. Briefly explain the causes of this gap. [RTP. MAY 2010]

Answer:

(a) The elements included in the 'Introduction' section of Information System Audit Report are as follows:

- **Context:** This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.

- **Purpose:** This sub-section is a short description of what functions and special programs were audited and the clients' authorities.

- **Scope:** The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.

- **Methodology:** This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.

(b) The causes of the gap identified between the need to protect the systems and the degree of protection applied, are as follows:

- Widespread use of technology,

- Interconnectivity of systems,

- Elimination of distance, time, and space as constraints,

- Unevenness of technological changes,

- Devolution of management and control,

- Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations, and

- External factors such as legislative, legal, and regulatory requirements or technological developments.

18. XYZ Company developed an information system for the integration of various organizational processes. The company wanted to sell this system as an ERP solution. But, any system has to possess few characteristics to qualify for a true ERP solution. What are those characteristics? Explain in brief. [RTP. NOV. 2010]

Answer:
These characteristics are given as follows:

☞ **Flexibility:** An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).

☞ **Modular & Open:** ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.

☞ **Comprehensive:** It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.

☞ **Beyond The Company:** It should not be confined to the organizational boundaries, rather support the on-line connectivity to the other business entities of the organization.

☞ **Best Business Practices:** It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organization.

19. ABC Technologies Ltd. is in the development of application software for various domains. For the development purposes, the company is committed to follow the best practices suggested by SDLC. SDLC provides the guidelines in terms of a sequence of activities. It consists of a set of steps and 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 to as deliverables.
A deliverable may be a substantial written document, a software artifact, a system test plan or even a physical object such as a new piece of technology that has been ordered and delivered. This feature of the SDLC is critical to the successful management of an IS project. Read the above carefully and answer the following:

(a) List the possible advantages from the perspective of an IS Audit.
(b) There are various advantages by following SDLC, but there are some shortcomings also. Briefly explain those shortcomings.
(c) Feasibility study is a key activity in the SDLC. What are the issues which are typically considered in the Feasibility Study?
(d) At the end of the analysis phase of SDLC, the system analyst prepares a document called 'Systems Requirements Specifications (SRS)'. Briefly explain the contents of a SRS. [RTP. NOV. 2010]

Answer:
(a) From the perspective of the IS Audit, the following are the possible advantages:

☞ The IS auditor can have clear understanding of the various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.

☞ The IS Auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.

☞ The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.

☞ The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

(b) Some of the shortcomings of the SDLC are as follows:

- ☞ The development team may find it cumbersome.
- ☞ The users may find that the end product is not visible for a long time.
- ☞ The rigidity of the approach may prolong the duration of many projects.
- ☞ IT may not be suitable for small and medium sized projects.

(c) The following issues are typically addressed in the Feasibility Study:

- ☞ Determine whether the solution is as per the business strategy.
- ☞ Determine whether the existing system can rectify the situation without a major modification.
- ☞ Define the time frame for which the solution is required.
- ☞ Determine the approximate cost to develop the system.
- ☞ Determine whether the vendor product offers a solution to the problem.

(d) Any SRS contains the following:

- ☞ **Introduction:** Goals and Objectives of the software context of the computer-based system; Information description.
- ☞ **Information Description:** Problem description; Information content, flow and structure; Hardware, software, human interfaces for external system elements and internal software functions.
- ☞ **Functional Description:** Diagrammatic representation of functions; Processing narrative for each function; Interplay among functions; Design constraints.
- ☞ **Behavioral Description:** Response to external events and internal controls.
- ☞ **Validation Criteria:** Classes of tests to be performed to validate functions, performance and constraints.
- ☞ **Appendix:** Data flow / Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- ☞ **SRS Review:** It contains the following :
  - ♦ The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.
  - ♦ The review reflects the development team's understanding of the existing processes. Only after ensuring that the document represents existing processes accurately, should the user sign the document. This is a technical requirement of the contract between users and development team / organization.

20. XYZ & Company is dealing in the information systems audit. The audit of an IS environment to evaluate the systems, practices and operations may include one or both of the following:

- ☞ **Assessment of internal controls within the IS environment to assure validity, reliability, and security of information.**
- ☞ **Assessment of the efficiency and effectiveness of the IS environment in economic terms.**

The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole. This includes evaluating

both the effectiveness and efficiency. The focus (scope and objective) of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness (result-orientation) and efficiency (optimum utilization of resources). Read the above carefully and answer the following:

(a) The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor. There is a set of skills that is generally expected from an IS auditor. Discuss those skills in brief.

(b) Explain various costs involved in the implementation and operation of controls.

(c) Discuss the controls to consider when reviewing the organization and management controls in an Information System.

(d) While reviewing the adequacy of data security controls, what are the items which need to be evaluated by an IS auditor? [RTP. NOV. 2010]

Answer:

(a) The set of skills that is generally expected from an IS auditor, include:

- Sound knowledge of business operations, practices and compliance requirements,
- Should possess the requisite professional technical qualification and certifications,
- An good understanding of information Risks and Controls,
- Knowledge of IT strategies, policy and procedure controls,
- Ability to understand technical and manual controls relating to business continuity, and
- Good knowledge of Professional Standards and Best practices of IT controls and security.

(b) Implementing and operating controls in a system involves the following five costs:

Initial setup cost: This cost is incurred to design and implement controls. For example, a security specialist must be employed to design a physical security system.

Executing cost: This cost is associated with the execution of a control. For example, the cost incurred in using a processor to execute input validation routines for a security system.

Correction costs: The control has operated reliably in signaling an error or irregularity, the cost associated with the correction of error or irregularity.

Failure cost: The control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses.

Maintenance costs: The cost associated in ensuring the correct working of a control. For example, rewriting input validation routines as the format of input data changes.

(c) The controls to consider while reviewing the organization and management controls in an Information system shall include:

Responsibility: The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.

An official IT structure: There should be a prescribed organization structure with all staff deliberated on their roles and responsibilities by written down and agreed job descriptions.

An IT steering committee: The steering committee shall comprise of user representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems, for example, the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.

(d) An IS auditor is responsible to evaluate the following while reviewing the adequacy of data security controls:

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

21. PQR Enterprises uses business continuity and disaster recovery plans in its various operations. Business continuity focuses on maintaining the operations of the 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 operation using a prioritized resumption list.
Read the above carefully and answer the following:

(a) In your opinion, what should be the goals of a business continuity plan?

(b) In the development of a business continuity plan, there are total eight phases; Business Impact Analysis is the third important phase. Discuss various tasks which are to be undertaken in this phase.

(c) There are various backup techniques available e.g. Full backup, Incremental backup, Differential backup, and Mirror backup. Describe differential backup technique in detail. [RTP. NOV. 2010]

Answer:

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

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

(b) A number of tasks are to be undertaken in this phase are given as follows:

- Identify organizational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize potential threats that may lead to a disaster.
- Identify critical business processes.
- Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
- Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
- Determine the maximum allowable downtime for each business process.
- Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
- Determine the impact to the organization in the event of a disaster, e.g. financial reputation, etc.

(c) Differential Backup: A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

22. RST Consultants is in the process of launching a new unit to provide various services to the organizations worldwide, to assist them right from the beginning i.e. from development to maintenance including strategic planning and e-governance areas. The company believes in the philosophy of green world i.e. uses papers to a minimum extent. COBIT is positioned to be comprehensive for management and to operate at a higher level than technology standards for information systems management. To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. In establishing the list of requirements, COBIT combines the principles embedded in existing and known reference models e. g. Quality Requirements, Fiduciary requirements, and Security Requirements.

Read the above carefully and answer the following:

(a) Explain various working definitions of COBIT.
(b) Describe the IT resources identified in COBIT.
(c) Discuss the Monitoring domain identified for the high level classification in COBIT framework. [RTP. NOV. 2010]

Answer:

(a) COBIT's working definitions are as follows:

- **Effectiveness:** It deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency:** It concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality:** It concerns the protection of sensitive information from unauthorized disclosure.
- **Integrity:** It relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **Availability:** It relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance:** It deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria.
- **Reliability of Information:** It relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

(b) The IT resources identified in COBIT can be explained / defined as follows:

Data: These are objects in their widest sense (i.e. external and internal), structured and nonstructured, graphics, sound, etc.
Application systems: These are understood to be the sum of manual and programmed procedures.
Technology: It covers hardware, operating systems, database management systems, networking, multimedia, etc.
Facilities: These are all the resources to house and support information systems.
People: It includes staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

(c) Monitoring: All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

23. ABC Technologies is a leading company in the BPO sector. Its most of the business processes are automated. The company is relying on Information Technology for information and transaction processing. The growth of E-commerce supported by the growth of the Internet has completely revolutionized and reengineered business processes. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate, it is reliable and no unauthorized disclosure of the same is made. Further, it is also presumed that the virtual business organization is up and running all the time on 24×7 basis. However, in reality, the technology-enabled and technology-dependent organizations are more vulnerable to security threats than ever before.

Read the above carefully and answer the following:

(a) Discuss the security objective of the organization.

(b) There are certain basic ground rules that must be addressed sequentially, prior to knowing the details of 'how to protect the information systems'. Explain those rules in brief.

(c) Describe various groups of management, comprised by security policy.
[RTP. NOV. 2010]

Answer:

(a) Security Objective: The objective of information system security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity, and availability".

For any organization, the security objective comprises three universally accepted attributes:

- **Confidentiality:** Prevention of the unauthorized disclosure of information.
- **Integrity:** Prevention of the unauthorized modification of information.
- **Availability:** Prevention of the unauthorized withholding of information.

The relative priority and significance of confidentiality, integrity and availability vary according to the data within the information system and the business context in which it is used.

(b) Prior to knowing the details of `how to protect the information systems', we need to define a few basic ground rules that must be addressed sequentially. These rules are:

- **Rule #1:** We need to know that 'what the information systems are' and 'where these are located'.
- **Rule #2:** We need know the value of the information held and how difficult it would be to recreate if it were damaged or lost.
- **Rule #3:** We need to know that 'who is authorized to access the information' and 'what they are permitted to do with the information'.
- **Rule #4:** We need to know that 'how quickly information needs to be made available should and it become unavailable for whatever reason (loss, unauthorized modification, etc.) '

(c) Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management:

- Management members who have budget and policy authority,
- Technical group who know what can and cannot be supported, and
- Legal experts who know the legal ramifications of various policy charges.

Information security policies must always take into account business requirements. Business requirements are the principles and objectives adopted by an organization to support its operations and information processing. E-commerce security is an example of such business requirements.

Furthermore, policies must consistently take into account the legal, statutory, regulatory and contractual requirements that the organization and its professional partners, suppliers and service providers must respect. The respect of intellectual property is a good example of such requirements.

24. 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, and documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations.

Read the above carefully and answer the following:

(a) 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. [RTP MAY. 2011]

Answer:

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

(b) Basic Principles of Waterfall Approach: These principles are given as under:

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

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

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

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

the business objectives will be achieved.

Read the above carefully and answer the following:

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

(b) Discuss data processing controls in brief.

(c) Briefly discuss auditors' role in application software acquisition/selection process.

(d) What are the costs involved in the implementation and operation of the controls? [RTP MAY. 2011]

Answer:

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

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

(b) Data processing controls are given as follows:

- Run-to-run totals: These help in verifying data that is subjected to process through different stages. If the current balance of an invoice ledger is Rs.150,000 and the additional invoices for the period is of total Rs.20,000 then the total sales value should be Rs.170,000. A specific record (probably the last record) can be used to maintain the control total.

- Reasonableness verification: Two or more fields can be compared and cross verified to ensure their correctness. For example, the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.

- Edit checks: Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.

- Field initialization: Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e., setting all values to zero before inserting the field or record.

- Exception reports: Exception reports are generated to identify errors in data processed. Such exception reports give the transaction code and why the particular transaction was not processed or what is the error in processing the transaction. For example, while processing a journal entry if only debit entry was updated and the credit entry was not up dated due to absence of one of the important fields, then the exception report would detail the transaction code, and why it was not updated in the database.

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

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

- To highlight risks before a vendor contract or a software agreement contract is signed.

- Ensure that the decision to acquire software should flow thorough feasibility study, vendor evaluation and RFP (Request for proposal) adequacy checked for.

- A RFP would include transaction volume, data base size, turnaround time and response time requirements and vendor responsibilities.

- The auditor needs to also check the criteria for pre-qualification of vendors and sufficient documentation available to justify the selection of the final vendor / product.

- The auditor may also collect information through his/her own sources on vendor viability, support infrastructure, service record and the like.

- Thorough review of the contract signed with the vendor for adequacy of safeguards and completeness. The contract should address the contingency plan in case of vendor failures such as, source code availability and third party maintenance support.

- To ensure that the contract went through legal scrutiny before it was signed.

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

(i) **Initial setup cost:** This cost is incurred to design and implement controls. For example, a security specialist must be employed to design a physical security system.

(ii) **Executing cost:** This cost is associated with the execution of a control. For example, the cost incurred in using a processor to execute input validation routines for a security system

(iii) **Correction costs**: If a control has operated reliably in signaling an error or irregularity, the cost associated with the correction of error or irregularity is termed as Correction Cost.

(iv) **Failure cost:** If a control malfunctions or not designed to detect an error or irregularity. These undetected or uncorrected errors cause losses, which is termed as Failure Cost.

(v) **Maintenance costs**: The cost associated in ensuring the correct working of a control. For example, rewriting input validation routines as the format of input data changes.

26. PQR Enterprises is engaged in a business of manufacturing electronic products. The company is in the process of automation of its various business processes. During this automation, technical consultant of the company suggested to perform the risk assessment activity and to mitigate the assessed risks. Basically, risk assessment seeks to identify 'which business processes and related resources are critical to the business', 'what threats or exposures exist, that can cause an unplanned interruption of business processes', and 'what costs accrue due to an interruption'. There are various analytical procedures that are used to determine various risks, threats, and exposures, faced by an organization. These are known as Business Impact Analysis (BIA), Risk Impact Analysis (RIA) and so on.

Read the above carefully and answer the following:

(a) Define Systematic Risks and Unsystematic Risks with the help of examples.

(b) There are various techniques that are available to assess and evaluate risks, namely, Judgment and Intuition, Delphi Approach, Scoring, Qualitative Techniques, and Quantitative Techniques. Explain Delphi and Scoring approaches in brief.

(c) In automation of the business modules, retention of electronic records is an important activity. How Information Technology (Amendment) Act 2008 addresses this issue with reference to its Section 7? [RTP MAY. 2011]

Answer:

(a) Systematic risks:

These are unavoidable risks; constant across majority of technologies and

applications. For example the probability of power outage is not dependant on the industry but is dependant on external factors. Systematic risks would remain, no matter 'what technology is used'. Thus effort to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Systematic risks can be reduced by designing management control process and does not involve technological solutions. For example, the solution to non availability of consumable is maintaining a high stock of the same. Thus a systematic risk can be mitigated not by technology but by management process. Hence, one would not make any additional payment for technological solution to the problem. That means there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

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

(b) Delphi Approach:

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

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

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

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

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

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

27. ABC Group of Industries is in the process of launching a new business unit viz. ABC

Consultants Ltd. to provide various consultancy services to the organizations worldwide, to assist them in the computerization of their business modules. It involves a number of activities starting from the capturing of the requirements to the maintenance. Business continuity and disaster recovery planning are two key activities in this entire process, which must be taken care right from the beginning. Business continuity focuses on maintaining the operations of an organization, especially the IT infrastructure in face of a threat that has materialized. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operations using a prioritized resumption list.

Read the above carefully and answer the following:

(a) What are the issues that are emphasized by the methodology for developing a business continuity plan?
(b) Explain the objectives of performing Business Continuity planning tests.
(c) What are the issues, written in a contract that should be ensured by security administrators if a third-party site is to be used for backup and recovery purposes? [RTP MAY. 2011]

Answer:

(a) The methodology for developing a business continuity plan emphasizes on the following:

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

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

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

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

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

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

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

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

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

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

(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 the following issues:

- 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.

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

Read the above carefully and answer the following:

(a) An ERP system is not only the integration of various organization processes. Any system has to possess few key characteristics to qualify for a true ERP solution. What are these features?

(b) 'Access Controls plays a key role in the implementation of information security policies'. Explain its detailed control and objectives.

(c) Describe 'Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security' with respect to the Section 69B of Information Technology (Amendment) Act, 2008.

(d) Briefly explain the tasks that are to be performed during the post-implementation period of an ERP package. [RTP MAY. 2011]

Answer:

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

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

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

- Business requirement for access control: To control access to information,
- User access management: To prevent unauthorized access to info systems,
- User responsibilities: To prevent unauthorized user access,
- Network access control: To protect of networked services,
- Operating system access control: To prevent unauthorized computer access,
- Application Access Control: To prevent unauthorized access to information held in information systems,
- Monitoring System Access and use: To detect unauthorized activities, and
- Mobile Computing and teleworking: To ensure information security when using mobile computing & teleworking facilities.

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

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub- section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

(d) Major tasks that are to be performed during the post-implementation of an ERP Package are given as follows:

- To develop the new job descriptions and organization structure to suit the post ERP scenario;
- To determine the skill gap between existing jobs and envisioned jobs;
- To assess training requirements, and create and implement a training plan;
- To develop and amend HR, financial and operational policies to suit the future ERP environment; and
- To develop a plan for workforce logistics adjustment.

29. XYZ Company, engaged in the manufacturing of several types of electronic goods is having its branches all over the World. The company wishes to centralize and consolidate the information flowing from its branches in a uniform manner across various levels of the Organization.

The factories are already working on legacy systems using an intranet and collating information. But each factory and branch is using different software and varied platforms, which do not communicate with each other. This not only results in huge inflow of data which

could not be consolidated for analysis but also the duplication of data. Even one percent change in any data entry or analysis translates into millions of Rupees and can sometimes wipe out the profits of the organization. So the company needs a system that would help them to be responsive and act fast.

Read the above carefully and answer the following with justifications:

(a) What are the problems that the company is facing now? (5 Marks)

(b) Should the company go for ERP solution? If yes, will the company be able to share a common platform with its dealers to access servers and database to update the information of issues of mutual interest? (5 Marks)

(c) For the selection of ERP package, state the issues to be considered. (5 Marks)

(d) Suggest how to go about the implementation of ERP package. (5 Marks)
[JUNE 2009]

Answer

(a) XYZ company, having its branches all over the world, is engaged in manufacturing of several types of electronic goods. It is confronted with the problem of centralizing and consolidating the information flowing in from its various branches in uniform manner across various levels of the organization.

No doubt, the factories are working on legacy systems using an intranet and collating information. As each factory is using different type of software on varied platforms, therefore, they are not able to communicate with each other. Because of this reason, there is a huge inflow of data which could not be consolidated for analysis. Lack of communication among factories has not only resulted into duplication of the data entry which is not only costly, slight change in data entry and analysis may translate into millions of rupees that can sometimes wipe out the profits of the organization . Hence, there is an urgent need of a system that would help the branches to be responsive and to act fast.

(b) Yes, the company should go for ERP solutions. ERP implementation brings different business functions, personalities, procedures, ideologies and philosophies on one platform, with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization. Some of the major features of ERP are that it provides the support to multi platform, multi facility, multi mode, manufacturing, multi currency, multi lingual facilities. It supports strategic and business planning activities, operational planning and execution activities, creation of material and resources. All these functions are effectively integrated for flow and updation of information immediately upon entry of any information, thereby providing a company- wide Integrated Information System.

In case, the company decides to include a module for dealers which provides limited/restricted access to company databases and server, dealers will be able to update the information of issues of mutual interest.

(c) While selecting the ERP package, the performance of following issues should be taken into account:

(i) Better inventory management and control.
(ii) Improved financial reporting and control.
(iii) Automation of certain takes that were performed manually to increase productivity.
(iv) Improved production planning.
(v) Better information on stocks at various locations.
(vi) Using an integrated system as opposed to disparate systems at different locations, thereby eliminating errors of duplicate entries.
(vii) More accurate costing of products.
(viii) Better credit control.
(ix) Improved cash flow planning.
(x) Automatic quality control and tracking.
(xi) Better after sales services.
(xii) Better information and reporting to top management.

(d) In the stated scenario, several steps involved in the implementation of a typical ERP package are enumerated below:

(i) Identifying the needs for implementing an ERP package.

(ii) Evaluating the 'As Is' situation of the business i.e., to understand the strength and weakness prevailing under the existing circumstances.

(iii) Deciding the 'Would be' situation for the business i.e., the changes expected after the implementation of ERP.

(iv) Reengineering the Business Process to achieve the desired results in the existing processes.

(v) Evaluating the various available ERP packages to assess suitability.

(vi) Finalizing of the most suitable ERP package for implementation.

(vii) Installing the required hardware and networks for the selected ER P package.

(viii) Finalizing the Implementation consultants who will assist in implementation.

(ix) Implementing the ERP package

30. A company is engaged in the stores taking data activities. Whenever, input data error occurs, the entire stock data is to be reprocessed at a cost of Rs. 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of Rs. 2,000 per stock taking period. The time taken for validation causes an additional cost of Rs. 200.

(i) Evaluate the percentage of cost - benefit effectiveness of the decision taken by the management and

(ii) suggest preventive control measures to avoid errors for improvement. (10 Marks) [JUNE 2009]

Answer:

(a) (i) The percentage of cost benefit effectiveness based on the information is calculated in the following table:

S. No.	***Particulars***	***Without validation Procedure***	***With Validation Procedure***
1.	Cost of reprocessing the stock data	Rs. 50,000	Rs. 50,000
2.	Risk of data errors Expected processing cost	12% Rs. 6,000	0.5% Rs. 250
	Cost of validation procedure	Nil	Rs. 2,000
3.	Cost of delay due to validation	Nil	Rs. 200
4.	**Total cost involved** Net expected benefit in %	**Rs. 56,000**	**Rs. 52,450**

Hence there is 6.3% cost benefit effectiveness of the decision taken by the management.

(ii) **Preventive Control Measures**

Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system. The broad characteristics of preventive controls are:

(i) A clear-cut understanding about the vulnerabilities of the asset.
(ii) Understanding probable threats.

(iii) Provision of necessary controls for probable threats from materializing.

Any control can be implemented in both manual and computerized environment for the same purpose. Only the implementation methodology may differ from one environment to the other.
Some of the major preventive controls to avoid errors are as follows:

- ⇨ Employ qualified personnel
- ⇨ Segregation of duty
- ⇨ Access controls
- ⇨ Vaccination against disease
- ⇨ Maintain proper documentation
- ⇨ Prescribing appropriate books for a course
- ⇨ Training and retraining of personnel
- ⇨ Authorization of transactions
- ⇨ Validation, edit checks in the application programs
- ⇨ Firewalls
- ⇨ Anti-virus software
- ⇨ Passwords

The above list in no way is exhaustive, but is a mix of manual and computerized preventive controls. The following table enumerates the kind of manual controls and computerized controls applied to a similar scenario.

Scenario	Manual Control	Computerized Control
Restrict unauthorized entry into the premises	Build a gate and post a security guard.	Use access control software, smart card, biometrics, etc.
Restricted unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorized person to use the applications.	Use access control, viz. User ID, password, smart card, etc.

31. The Information Security Policy of an organization has been defined and documented as given below:

"Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes."

Identify the salient components that have not been covered in the above policy. (5 Marks) [JUNE 2009]

Answer:
A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization.

An information Security policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

Issues to address: This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

- ⇨ a definition of information security,

- ⇨ reasons why information security is important to the organization, and its goals and principles,

⇨ a brief explanation of the security policies, principles, standards and compliance requirements,

⇨ definition of all relevant information security responsibilities, and

⇨ Reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should re view any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

In the stated scenario of the question, the ISMS Policy of the given organization does not address the following issues:

(i) Definition of information security,
(ii) Reasons why information security is important to the organization ,
(iii) A brief explanation of the security policies, principles, standards and compliance, and
(iv) Reference to supporting documents.

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

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

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

Read the above carefully and answer the following with justifications:

(a) To overcome the problems which the financial analysts are facing, what kind of software the company should select? (10 Marks)

(b) The company is advised that the adoption of BS7799 International Standard will help in overcoming the problems and achieving its goals. Discuss. (5 Marks)

(c) How should the human resources be enriched for effective utilization of the proposed new systems and standards? [NOVEMBER 2009] (5 Marks)

Answer:

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

⇨ Missing the access to the same data as well as timely access to information.

⇨ Dated budget and actual numbers for each business unit reside in seven different systems, separating critical components of the profit and loss account thus failing the financial analysts to assess results.

⇨ The field analysts are not able to retrieve the data themselves from one universal place and therefore they have to rely upon the home office for the same.

It is therefore important that the company should buy new software for the solution of the problems as mentioned above.

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

- ⇨ hands on ability to consolidate budgets, based on actual data in the process,
- ⇨ enabling business units to make real-time, online decisions based on more accurate information,
- ⇨ user friendly.

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

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

The company can use BS 7799 for the following reasons:

- ⇨ Reduced operational risk,
- ⇨ Increased business efficiency, and
- ⇨ Assurance that information security is being rationally applied. This is achieved by ensuring that:
- ⇨ Security controls are justified.
- ⇨ Policies and procedures are appropriate.
- ⇨ Security awareness is good amongst staff and managers.
- ⇨ All security relevant information processing and supporting activities are auditable and are being audited.
- ⇨ Internal audit, incident reporting / management mechanisms are being treated appropriately.
- ⇨ Management actively focuses on information security and its effectiveness.

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

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

experts need training organized by the vendor through hands-on learning techniques.

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

- ⇨ **User training:** User training deals with the operation of the system itself. Training in data coding emphasizes the methods to be followed in capturing data from transactions or preparing data for decision support activities. Users should be trained on data handling activities such as editing data, formulating inquiries (finding specific records or getting responses to questions) and deleting records of data. From time to time, users will have to prepare disks, load paper into printers, or change ribbons on printers. Some training time should be devoted to such system maintenance activities. If a micro computer or data entry system uses disks, users should be instructed in formatting and testing disks. It is also required to have managers directly involved in evaluating the effectiveness of training activities because training deficiencies can translate into reduced user productivity level.

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

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

(a) What are the two primary methods through which the analyst would have collected the data? (5 marks)
(b) To achieve their objectives, what are the points BS 7799 has to ensure? (5 marks)
(c) Suppose an audit policy is required, how will you lay down the responsibility of audit? (5 marks)
(d) To retain their e-documents for specified period, what are the conditions laid down by Section 7, Chapter III of Information Technology Act, 2000? (5 marks)

Answer:

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

(1) **Reviewing internal documents:** The analyst first tries to learn about the organization involved in or affected by the project. For example, to review an inventory system proposal, s/he will try to know 'how the inventory department operates' and 'who are the managers and supervisors'. S/he will examine organization charts and written operating procedures.

(2) **Conducting interviews:** Written documents tell the analyst 'how the system should operate' but they may not include enough details to allow a decision to be made about the merits of a system proposal nor do they present users' views about current operations. To learn these details, analysts use interviews. Preliminary investigation interviews involve only management and supervisory personnel.

(b) BS 7799 should ensure that:

(1) Security controls are justified.

(2) Policies and procedures are appropriate.

(3) Security awareness is good amongst staff and managers.

(4) All security relevant information processing and supporting activities are auditable and are being audited.

(5) Internal audit, incident reporting/management mechanisms are being treated appropriately.

(6) Management actively focuses on information security and its effectiveness.

(7) Certification can also be used as a part of marketing initiative, providing assurance to business partners and other outsiders.

(c) The scope of information system auditing should encompass the examination and evaluation of the adequacy and effectiveness of the system of internal control and the quality of performance by the information system. Information System Audit will examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists that objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The audit policy should lay down the responsibilities as follows:

(1) The policy should lay out the periodicity of reporting and the authority to whom the reporting is to the made.

(2) A statements of professional proficiency may be included to state the minimum qualification and experience requirements of the auditors.

(3) All information system auditors will sign a declaration of fidelity and secrecy before commencing the audit work in a form that the inspection department may design.

(4) The policy may lay out the extent of testing to be done under the various phases of the audit like Planning, Compliance Testing, and Substantive Testing.

(5) A documented audit program would be developed including the following:

- ♦ Documentation of the information system auditor's procedures for collecting, analyzing, interpreting, and documenting information during the audit.
- ♦ Objectives of the audit.
- ♦ Scope, nature, and degree of testing required for achieving the audit objectives in each phase of the audit.
- ♦ Identification of technical aspects, risks, processes, and transactions which should be examined.
- ♦ Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.

(6) The policy should determine when and to whom the audit results would be reported and communicated. It would define the access rights to be given to the auditors.

(7) The Policy should outline the compliance testing areas.

(8) The auditor will carry out substantive testing wherever the auditor observes weakness in internal controls or where risk exposure is high. The auditor may also carry out such tests to gather additional information necessary to form an audit opinion.

(9) The Audit Policy would define the compulsory audit working papers to be maintained and their formats.

(d) Section 7, Chapter III of Information Technology Act, 2000/ Information Technology (Amendment) Act, 2008 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

(i) The information therein remains accessible so as to be usable subsequently.

(ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.

(iii) The details which will facilitate the identification of the origin, destination, dates and time of dispatch or receipt of such electronic record are available therein.

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

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

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

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

(a) When the existing information system is to be converted into a new system, what are the activities involved in the conversion process? (5 Marks)

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

(c) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity. (5 Marks)

(d) What is the procedure to apply for a license to issue electronic signature certificates, under Section 22, Information Technology (Amendment) Act, 2008? (5 Marks) [NOV. 2010]

Answer:

(a) Conversion from existing information system to a new system involves the following activities:

(i) Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually';

(ii) Performing data cleansing before data conversion;

(iii) Identifying the methods to assess the accuracy of conversion like record counts and control totals;

(iv) Designing exception reports showing the data which could not be converted through software; and

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

(b) Types of Operations:

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

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

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

(c) Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

(i) **Business resumption planning** – The Operation's piece of business continuity planning;

(ii) **Disaster recovery planning** – The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.

(iii) **Crisis Management** – The overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

(d) Procedure to apply for a license to issue electronic signature under Section 22, IT (Amendment) Act, 2008 is given follows:

1. Every application for issue of a license shall be in such form as may be prescribed by the Central Government.
2. Every application for issue of a license shall be accompanied by

(i) a certification practice statement;
(ii) a statement including the procedure with respect to identification of the applicant;
(iii) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government; and
(iv) Such other documents, as may be prescribed by the Central Government.

35. As a person in-charge of System Development Life Cycle, you are assigned a job of developing a model for a new system, which combines the features of a prototyping model and the waterfall model. Which will be the model of your choice and what are its strengths and weaknesses?

(8 Marks) [NOV. 2010]

Answer:

As a person in-charge of system development life cycle, the spiral model will be the choice. The spiral model is a software development process, combining elements of both design and prototyping-in-stages, in an effort to combine/ advantages of top-down and bottom-up concepts. It is a system development method, which combines the features of the prototyping model and the waterfall model. The spiral model is intended for large, expensive and complicated projects. Its major distinctiveness is given as follows:

(i) The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.

(ii) A preliminary design is created for the new system. This phase is the most important part of 'Spiral Model' in which all possible alternatives that can help in developing a cost effective project are analyzed and strategies are decided to use them. This phase has been added specially in order to identify and resolve all the possible risks in the project development. If risks indicate any kind of uncertainty in requirements, prototyping may be used to proceed with the available data and find out possible solution in order to deal with the potential changes in the requirements.

(iii) A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.

(iv) A second prototype is evolved by a fourfold procedure:

- ⇨ evaluating the first prototype in terms of its strengths, weaknesses, and risks;
- ⇨ defining the requirements of the second prototype; planning and designing the second prototype; and constructing and testing the second prototype.
- ⇨ Game development is a main area where the spiral model is used and needed, that is because of the size and the constantly shifting goals of those large projects.

Strengths:

(i) Enhance risk avoidance;
(ii) Useful in helping to select the best methodology to follow for development of a given software iteration based on project risk.
(iii) Can incorporate waterfall, prototyping and incremental methodologies as special cases in the framework, and provide guidance as to which combinations of these models best fits a given software iteration, based upon the type of project risk.

Weaknesses:

(i) Challenges to determine the exact composition of development methodologies to use for each iteration around the spiral.
(ii) Highly customized to each project and thus is quite complex, limiting reusability.
(iii) A skilled and experienced project manager required to determine how to apply it to any given project.
(iv) No established controls for moving from one cycle to another cycle. Without controls, each cycle may generate, more work for the next cycle.
(v) No firm deadlines cycles continue with no clean termination condition, so there is an inherent risk of not meeting budget or schedule.

Compiled by: Keshav Arya
E-mail: keshav_arya@yahoo.com
Source: ICAI RTP, Past Question Papers

Problems from Mr. DINESH MADAN

Question - 1:

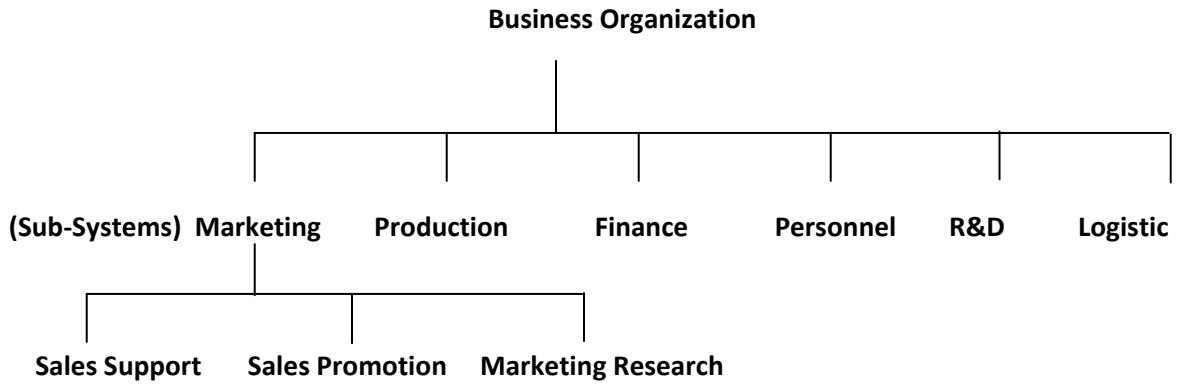
As a member of the system development team, explain the process of decomposition of an organization into various functional blocks to comprehend the information processing system with the help of an example:

Answer -1:

Any system can be divided into smaller systems known as sub-systems and a sub-system can further be divided into smaller systems known as sub-sub-system. ***The process of dividing the system into smaller systems is known as system decomposition.***

This process continues until the smallest sub-systems are of manageable size. The concept of sub-system is an important aspect and considered as basis for analysis and design of information systems, because it is difficult to manage a complex system when considered as whole. Therefore, for the sake of convenience and clarity, a system is divided into smaller systems. The process of dividing or factoring a system into smaller system is known as decomposition. The sub-systems resulting from this process usually form hierarchical structures. In a hierarchy, a sub-system is one element of a ***supra-system*** (the system above it).

The figure below provides decomposition of organization various functional blocks, which ultimately get converted into information sub-systems.



System Decomposition

Question - 2:

An organization is in the stage of systems development to implement an enterprise wide information system, where the following conditions exist:

The new system is mission critical and there is hasty need
End users are not aware of the information needs

The business risks associated in implementing the wrong system are high
Read the above case carefully and answer the following with proper justifications:

(a) Indetify the system development approach and steps to be followed in the above stated conditions.
(b) State the reasons for choosing the particular approach for system development
(c) Indentify the risks, when end-users are involved in the system development process.

Answer -2:

There are three important elements in the above case

(1) System is immediately required
(2) End user involvement is required at high level because users are not aware of the information needs
(3) The business risks of implementing wrong system are high

Based on these elements, given below are the answers to the questions raised in the above case.

(a) Considering the above conditions, I would suggest to use the RAD (Rapid Application Development) approach. The key objective of this approach is fast development of high quality system.

(b) There are many reasons for selection of this approach:

- Provides quick development of required information system
- Allows incremental prototyping which help to understand users requirements better.
- Allows the extensive involvement of end users through Joint application development (JAD) workshops which reduces the risks of wrong system implementation
- Allows the use of CASE (Computer Aided Software Engineering) tools which help to develop mission critical applications with high quality

(c) Normally, end-users involvements help to develop right system; however, end-users involvement may cause the following risks:

- End-users involved are not knowledgeable enough to provide the right suggestions, this may cause system is developed with wrong specifications
- End-users involved are not given adequate delegations which may cause delay in decision making

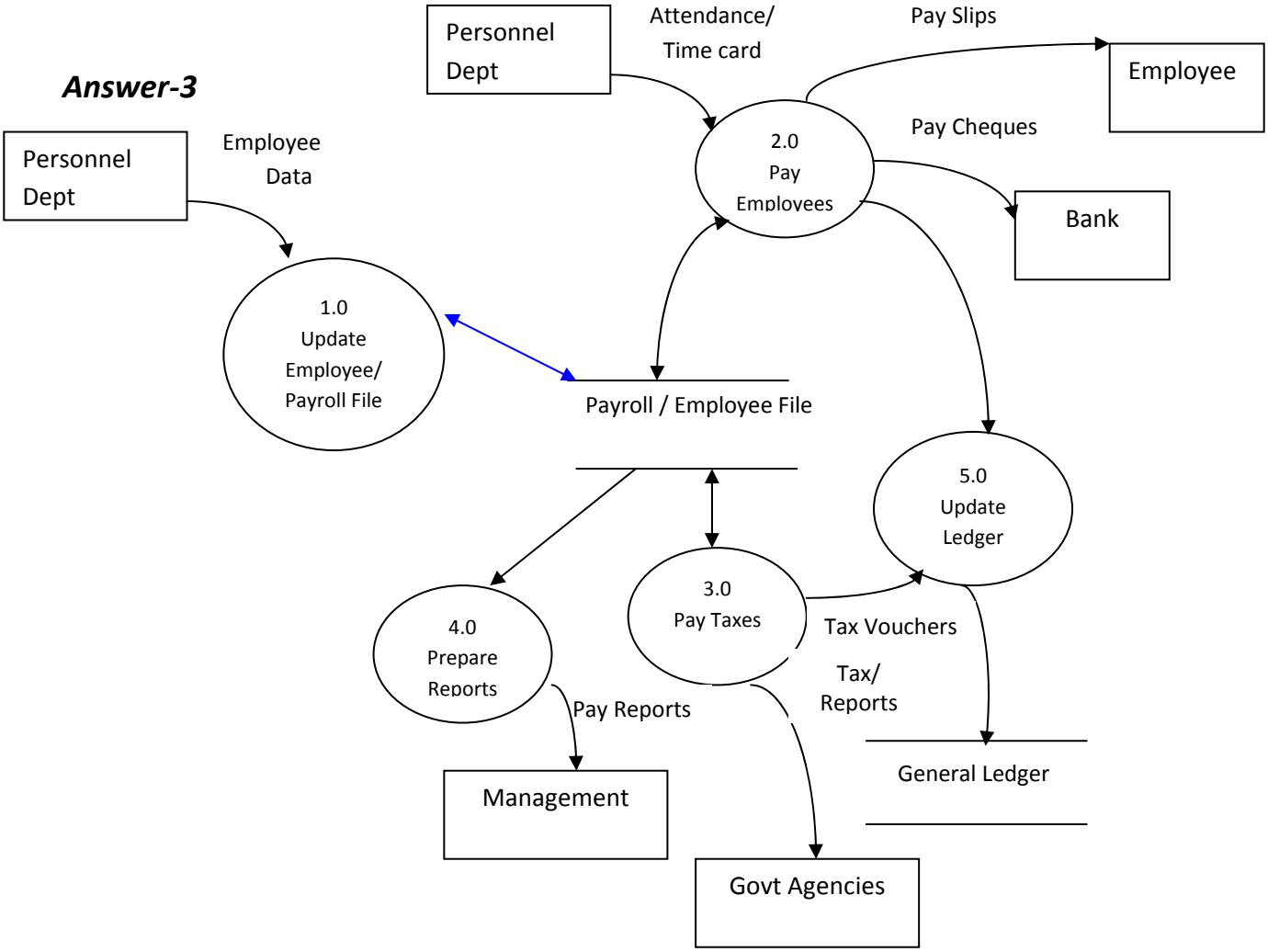
Question - 3:

Read the data flow and activities listed in the table below carefully and draw the data flow diagram for the payroll processing system.

Activities	**Data inputs**	**Data output**
Update employee/ roll file	New employee form Employee change form Employee/pay roll file	Update employee/ pay roll

Pay employees	Time cards Employee/pay roll file Tax table	Employee cheques Pay roll register update employee/ pay roll file pay roll cheques pay roll cash disbursements voucher
Prepare reports	Employee / pay roll file	Pay roll reports
Update general ledger	Payroll tax cash disbursements voucher pay roll cash disbursements voucher	Update general ledger

Answer-3



DFD for Payroll Processing (Level-1)

Question-4:

As a system analyst, you need to assess the successful implementation and stake holder's actual requirement of an enterprise system in retail chain organization across its braches to provide the following features:

- Lower operational costs,
- Better information for managers, and
- Smooth operation for users or better levels of service to customers.

Justify your answer with the necessary techniques used to determine the requirement of a system:

Answer -4:

System analysis is very important phase of system development, since any error in this phase would affect all subsequent phases of development. The aim of the system analysis phase is to thoroughly understand the user requirements and remove any inconsistencies and incompleteness in these requirements. This phase help to design the system with best possible features as mentioned above in the question i.e. lower operational cost, better information for managers and smooth operation for users or better levels of service to customers:

The following techniques can be used to determine the requirements from the systems:

(1) Collection of Detail Information: In this step, detail information about the requirement from the new retail system will be collected. The following fact finding techniques can be used for information collection:

(a) Review and collection of documents being used in the retail chain

(b) Interview with users

(c) Questionnaire for users to provide response to set of questions incase users can not provide time for interview

(d) Personal Observations of users working

(2) Analysis of the Existing System: In this step, the analysts perform a detail analysis of users' existing system which in turn helps to define the users' requirements from the proposed system in a better manner.

(3) System Analysis of Proposed System: Once the analysis of existing system is completed, the analysis of the proposed system starts. The proposed system analysis is done by using the data collected in "Collection of Detail Information" step and models prepared during the "Analysis of Existing System".

With the above analysis the analysts can design the system which can provide the following features:

- Lower operational costs,
- Better information for managers, and
- Smooth operation for users or better levels of service to customers.

Question-5.

An auditor while evaluating the reliability of a control implemented in a transaction process had to estimate the reliability per transaction. A test was undertaken and result indicated that control was unreliable. The reliability of the process was 0.15 when control was in place and was 0.09 when the control was absent. The management had estimated the cost of reprocessing the errors as Rs.1000 per transaction procedure. Evaluate the net benefit of the control procedure if the cost implementation of the control is Rs. 10,000.

Answer-5:

It seems this question is not clearly defined in the practice manual but I am providing the possible answer for this:

Cost of reprocessing an error	= Rs. 1000
Chances of error without control	= 1- 0.09
	= 0.91
Therefore, expected error cost without control	= 1000*0.91
	= Rs. 910
Cost of implementing the control	= Rs 10,000
Chances of error with control	= 1 – 0.15
	= 0.85
Therefore, expected error cost with control	= 1000*0.85
	=Rs. 850
Net benefit per transaction with control	= 910 – 850
	= Rs. 60

The system will achieve benefits with control if more than =10000/60

=167 transactions will have errors

Question-6:

A company is engaged in the stores stock taking data activities. Whenever, input data error occurs, the entire stock data is reprocessed at a cost of Rs. 50,000. The management has decided to introduce a data validation step that would reduce errors from 12% to 0.5% at a cost of Rs.2,000 per stock taking period. The time taken for validations causes an additional cost of Rs. 200

(i) Evaluate the percentage of cost-benefit effectiveness of the decision taken by the management and

(ii) Suggest preventive control measures to avoid errors for improvements

Answer-6:

(i) Evaluate the percentage of cost-benefit effectiveness of the decision taken by the management

Without Control:

Chances of Error	=12%
Cost of one error	= Rs. 50,000

Expected cost of error	=Rs. 12% * 50,000
	=Rs. 6,000

With Data Validation Control:

Chances of Error:	=0.5%
Cost of one Error	=Rs. 50,000
Expected cost of error	=Rs.0.5% * 50,000
	=Rs. 250
Cost of per stock taking with control	=Rs. 2000
Additional cost per stock taking	=Rs. 200

Total expected cost with data validation control= Rs. 2,450

Percentage of cost-benefit

Benefit with data validation	= 6,000- 2,450 = Rs. 3,550
Benefits % with data validation	= (3550/6000)
	=60%

(ii) Suggest preventive control measures to avoid errors for improvements

Preventive Controls:

These controls as name suggest are designed to prevent an error or any malicious activity in the system, for example using login-id and password is a preventive control. Preventive controls are implemented for both computerized and manual environment; but techniques and implementation may differ depending upon the type of threats and exposure. Below list provides some examples of preventive controls.

- Employ qualified personnel
- Segregation of duties
- Proper Documentation
- Authorization of transactions
- Validation of transactions through various checks

Question -7:

Identify and briefly discuss the necessary data integrity control techniques for the following processes in a payroll system:

(a) addition/deletion/updating of employee data by the HR department:

b) Payroll processing and storage

(c) Pay-slip generation and consolidated pay-report department wise

Answer -7:

Hint:

(a) Describe input/source document controls of data integrity

(b) Describe processing and storage controls of data integrity controls

(c) Describe output controls of data integrity controls

Question -8:

A retail company has been in the process of converting its manual sales into a computerized system with the implementation of a Point of Sales system for the last 6 months. The company needs to evaluate the software application system for its completeness, correctness and quality.

Read the scenario carefully and answer the following:

(a) State the test plant to be performed to check if the different modules of the application are integrated seamlessly
(b) Indentify the testing method to verify that the application is efficient to handle about 500 POS counters concurrently
(c) Explain the testing method used to test the consistency between different versions of the same application.

Answer -8:

(a) ***The test plan for this task will be "INTEGRATION TEST PLAN":***
In this test plan, functionalities which link one unit with another are tested. This test plan includes activities for testing of integrated functionalities.

(b) For this we will use two testing methods:
(1) Volume Testing: It is the testing of the system to check whether system will work efficiently when 500 POS counters will be simultaneously active and when the database contains the greatest data volume load.
(2) Stress Testing: This testing helps to determine how many numbers of POS can be simultaneously active without compromising the system performance.

(c) For this we will use a testing method known as regression testing (you can read about this from reference book)

Question -9:

An automobile spare parts production company has 10 distribution centers, each of which maintain their inventory status through the company's inventory application software on its Virtual Private Network (VPN). Managers across the distribution centers have identified different types of frauds / errors committed during data entry, transaction processing and fake users' logins in the inventory system.
The managers on one of the distribution center has asked you (IS auditor) to prepare a report on "how the risk appraisal can be undertaken". Indicate the appropriate approach in this situation and give reasons for your answers.

Answer-9:

Here the major problem is frauds committed during data entry and transaction processing. Also, the fake users login into the inventory system. These problems seem to be due to absence of adequate controls and security policy. In the risk appraisal of these problems the following approach can be mentioned by auditor:

- Identification of types errors and frauds in the system.

- Determination of possible losses due to these errors and frauds in the systems
- Review of existing applied controls and security policy to avoid these errors and frauds (which seem to be inadequate)
- Identification of types of controls which can be applied to avoid these frauds and errors
- Cost of implementation of these controls vs. benefits from controls
- Implementation of controls
- Monitoring/review of applied controls for potential corrections
- Suggestion to develop and implement an effective information security policy

Question -10:

Briefly explain the control measures to ensure confidentiality, integrity, and availability of data.

Answer - 10:

Please explain in this the below 10 domains of BS 7799 or Focus area of ISMS

- *SECURITY POLICY*
- *ORGANISATIONAL SECURITY*
- *ASSET CLASSIFICATION & CONTROL*
- *PERSONNEL SECURITY*
- *PHYSICAL AND ENVIRONMENTAL SECURITY*
- *COMMUNICATIONS AND OPERATIONS MANAGEMENT*:
- *ACCESS CONTROL*
- *SYSTEM DEVELOPMENT AND MAINTENANCE*
- *BUSINESS CONTINUITY MANAGEMENT*
- *COMPLIANCE*

Question-11:

A backup plan is to be prepared for XYZ company in order to specify the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making a backup, location of backup resources, sites where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recover various systems and a time frame for the recovery of each system. But the most difficult part in preparing the backup plan is to ensure that all the critical resources are backed up. List the resources that are to be considered in a backup plan.

Answer: -11:

Backup plan is the most crucial plan for immediate recovery from disaster. Backup plan is considered as a supportive plan for the recovery plan. In this plan, as mentioned above various planning related to type of backup, frequency of backup and location of backup etc are decided and implemented.

In general, the following resources are considered for backup

- Personnel: Arrangement of staff to maintain information system in any emergency and also arrangement with another company for provision of staff.
- Hardware: Arrangement of backup/standby hardware
- Facilities: Arrangement of standby facilities or arrangement with another company for provision of facilities
- Documentation: Inventory of documents also at some off-site location
- Data/Information: Backup of data files at on-site, as well at off-site locations
- Application Software: Inventory of application software at on-site, as well at off-site locations
- System software: Inventory of application software at on-site, as well at off-site locations

Question: 12

ABC limited has migrated from traditional system to new real time integrated ERP systems. The technical advisor of the company advised to the owner that the company should take necessary steps to analyze several types of risks. Explain those risks in brief.

Answer: 12

Migration to real-time and integrated ERP system, from old system, is not an easy process. It involves many risks and governance issues; such as:

Risks and Issues with ERP:

Single Point Failure: ERP provides an integrated system in the organization which is managed by a single ERP application (software). Failure of ERP application/main-server may bring down the working of entire organization's information system.

Change Management: ERP implementation is not only an implementation of a computer based integrated system; it requires changes in existing processes, culture and working methods of organizations' staff/stakeholders. And adapting to new processes, culture and working method for staff is always a big challenge.

Structural Changes: Not only the implementation of ERP requires change in processes and working methods; it also requires the structural changes (re-arrangement of departments) in the organization through BPR to achieve the best practices.

Job Profile Changes: The change management and structural changes may need the change in job profiles of the staff from existing job profiles. This is also a very big risk and governance issue, as staff normally resist for change in their job profiles.

On-line and Real-time System: ERP provides an on-line and real-time data processing system which requires a continuous maintenance capability, and also requires a quick response to any system problems and new requirements. Maintaining such capabilities is always a big challenge for the organizations.

Distributed Computing: ERP provides a distributed data processing system, which helps to process data from anywhere. Inexperience with distributed computing implementation and management also put forward a big challenge.

Dependence on External Assistance: Previously, organizations used to manage information system through internal support only. But ERP management requires the support of external assistance and that may expose for security and resource management risks to organizations data and resources.

Program Interfaces and Data Conversions: ERP requires extensive interfaces with other systems (like banks, tax authorities, customers and suppliers' systems), and it also requires extensive data conversion from old (legacy) system. These tasks always pose a big challenge to organizations**.**

Audit expertise: ERP environment require expertise to implement the controls and audit those controls.

Single sign on: A single sign-in to ERP system provides access to multiple modules and applications which create a security problem to the organizations.

Data Content Quality: ERP system requires the data inputs from multiple external data sources like customers, suppliers and banks. This may affect the data quality in the system.

Privacy and Confidentiality: There is risk of disclosure of personnel information to greater extent as ERP systems are connected with multiple external data sources.

Question:-13

What is enterprise controlling? Briefly explain its modules:

Answer:-13

ERP provides a module known as ***Enterprise Controlling*** which helps to manage and control entire Enterprise in an integrated manner. This module contains accounting data prepared by subsidiaries for corporate reporting which is automatically prepared within the local books of each subsidiary but consolidated at corporate level.

This data is transferred to a module called Enterprise Controlling (EC).

Date transfer to EC module automatically set up consolidated financial statements including elimination of inter-company transactions, currency translation etc.

Enterprise Controlling consists of 3 modules.

1. EC-CS: This allows the financial consolidation at corporate level.
2. EC-PCA: Implement transfer pricing rule for inter companies transactions
3. EC-EIS: Provide KPI (key performance indicators) at corporate levels to top-executive

Enterprise Controlling allows to control the whole enterprise from a corporate and a business unit perspective within one common infrastructure. It helps to speed up provision of business control information by fully automated corporate reporting from operative accounting via financial consolidation to management reporting. From EC-EIS top-level reports, end users can drill down to more detailed information within EC or any other SAP-R/3 application. EC can work with data from SAP and non-SAP sources.

Question-14

A company is developing several types of biscuits having its branches all over the country. The owner of the company wishes to centralize and consolidate the information flowing from its branches in a uniform manner across various levels of the organization. The technical advisor of the company recommended that the company should go for the implementation of the ERP package. Why the company should undertake ERP?

Answer-14

If we look at the broad perspective that why companies undertake the ERP then those can be the followings:

Integrate financial information:
Because the operation of company is located at different locations and if the owner tries to understand the company's overall financial performance, he may find the differences in the outputs given by different units and departments. For example, finance may have its own set of revenue numbers, sales may have another set, and the different business units may each have their own set for how much they contributed to revenue. ERP creates a single set of numbers that cannot be questioned because everyone is using the same system.

Integrate customer order information:
ERP systems can help to integrate the customer order information irrespective of the place from where order is inserted and executed. By having this information in one software system, rather than scattered among many different systems that can't communicate with one another helps to keep track of orders more easily, and coordinate manufacturing, inventory and shipping among many different locations simultaneously.

Standardize and speed up manufacturing processes:
Manufacturing companies-especially those with an appetite for mergers and acquisitions—often find that multiple business units across the company make the same transaction/ recording/ report using different methods and computer systems. ERP systems come with standard methods for automating some of the steps of a manufacturing process. Standardising those processes and using a single, integrated computer system can save time, increase productivity and reduce headcount.

Reduce inventory:
ERP helps the manufacturing process flow more smoothly, and it improves visibility of the order fulfilment process inside the company. That can lead to reduced inventories of the materials used to make products (work-in-progress inventory), and it can help users better plan deliveries to customers, reducing the finished good inventory at the warehouses.

Standardise HR information:
Especially in companies with multiple business units, HR may not have a unified, simple method for tracking employees' time and communicating with them about benefits and services. ERP can fix that.

Question-15:

Explain the relevance of BS 7799 (ISO 17799) for Indian Companies:

Answer-15

In the recent past, Indian companies and the Government have invested heavily in the IT infrastructure. However, theft of data and attacks on Indian sites and companies are alarming. Attacks and theft that happen on corporate websites are high and is usually kept under "strict" secrecy to avoid embarrassment from business partners, investors, media and customers. Huge losses are sometime remained un-audited and the only solution is to involve a model where one can see a long-run business led approach to Information Security Management.

BS 7799 (ISO 17799) consists of 127 best security practices (*covered under the 10 Domains which are discussed in chapter-8*) which Indian companies can adopt to build their Security Infrastructure. Even if a company decides not go in for the certification, the BS 7799 (ISO 17799) model helps companies maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. Additional benefits of ISMS are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact. Ultimately these factors lead to increased profitability.

The 10 domains of BS 7799 or Focus Area of ISMS (Information Security Management Systems)

- *SECURITY POLICY*
- *ORGANISATIONAL SECURITY*
- *ASSET CLASSIFICATION & CONTROL*
- *PERSONNEL SECURITY*
- *PHYSICAL AND ENVIRONMENTAL SECURITY*
- *COMMUNICATIONS AND OPERATIONS MANAGEMENT*:
- *ACCESS CONTROL*
- *SYSTEM DEVELOPMENT AND MAINTENANCE*
- *BUSINESS CONTINUITY MANAGEMENT*
- *COMPLIANCE*

Question-16:

ABC Company is implementing the health insurance portability and accountability act (HIPPA). There is a security rule issued under the act which lays out three types of security safeguards required for compliance. What are those conditions under these safeguards for which the company should look after?

Answer -16:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the USA promises to streamline the conduct of electronic healthcare transactions by imposing standards, and at the same time to ensure the integrity, confidentiality and availability of the individually identifiable health information involved.

There are two HIPAA titles:

Title I

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II

- **Title II** of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions
- **Title –II also requires** national identifiers for health services providers, health insurance plans, and employers.
- The AS provisions also address the security and privacy of health data.
- The standards are meant to improve the efficiency and effectiveness of the US health care system by encouraging the widespread use of electronic data interchange in the US health care system.

For us the topic of interest here is the Security Rule issued under the Act

The Security Rules:

- The Security rules lays out three types of security safeguards required for compliance: administrative, physical, and technical.
- For each of these types, the rules identify various security standards.
- And for each standard, there are both required and addressable implementation specifications.
- Required specifications must be adopted. Addressable specifications are more flexible. Individual entities can evaluate their own situation and determine the best way to implement addressable specifications.

HIPPA security rules requires three types of security safeguards:

- **Administrative Safeguards**
- **Physical Safeguards**
- **Technical Safeguards**

Administrative Safeguards:

- The use of administrative procedures for security include Certification, Contingency plans, Internal audit procedures, Security management process
- Training and awareness among staff for effective use of system.
- Documentation of processes used to protect data.
- Rules are required to manage the conduct of the personnel in relation to protection of the data.

Physical Safeguards:

- There should be procedures for protecting the physical computers systems and building containing data from fire, intrusion and any form of physical damage.
- Workstations should be used in such a way to avoid their direct access or view from users
- The movement of media/devices (containing data) in and out should be in a secured manner

Technical Safeguards:

- There should be processes in place for protecting information and to control individual access of such information.

By using

- Access Control.
- Authorization Control
- Audit Control.
- Message Authentication

Question-17:

Briefly discuss end user computing policies with respect to a sample IS security policy:

Answer -17:

The Information System (IS) security policy is a set of laws, rules, and practices that regulates how information is managed, protected, and distributed within an organization.

There are different categorizations of Information System security policy:
(1) Organization Security Policy
(2) User Policies
(3) Conditions for connection

User computing policies consist of a “User Security Policy” and “Acceptable Usage Policy”.

User security Policy set out the responsibilities and requirements for IT system users. For example:

- User will be provided a unique ID
- User will use a strong password for access of system
- User will not share his/her password with other users and outsiders
- User will not use the office system for personal work
- Games may not be stored or used on computer system
- Storage of sensitive Information on Personal Computers (PCs) must be protected through encryption techniques to restrict the viewing of information to authorized users only; and through lock in key for physical protections.

Acceptable Usage Policy provides acceptable use of internet access and email. For example:

- Organization will not allow the users to use office email for personal communications.
- Internet access will be permitted only for official work.

- Any content which is obscene or sexual in nature will not allow to be downloaded into the office system.
- User can not visit the prohibited sites.
- Users not following the acceptable usage policy may be fired from the organization.

Question-18:

Differentiate between the responsibilities of a Facilities Management Security Officers and Divisional System Security Officers with respect to organizational security structure.

Answer-18:

Facilities Management Security Officer (FMSO): The Facilities Management Security Officer (FMSO) reports directly to Facilities Management (or Facilities Managers) on all security matters relating to personnel. The role involves ensuring the controls are implemented, adhered to and reviewed as necessary.

Divisional System Security Officer (DSSO): A System Security Officer (SSO) from each division will be appointed as a DSSO. The SSO is a senior person appointed to fulfill the role of System Security Officer (SSO) for each ***major application system*** or **group of *systems.*** SSO responsibilities focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.
The DSSO carries the same responsibilities as a SSO and in addition is responsible for representing the SSOs in their division at the ISMG (Information Security Management Group) and for communicating requirements and issues to/from this group.

Question-19:

It is clear from various instances that there are not only many direct and indirect benefits from the use of information systems, but many direct and indirect risks related to the use of information system. These risks have led to a gap between need to protect systems and the degree of protection applied. Briefly explain the causes of this gap.

Answer-19:

Risk: Risk is a probabilistic terms, it is likelihood that an organization may be exposed to some threats that may cause harms to organizations. For example, organizations are exposed to risks of fire and theft etc so fire and theft are the risks to organizations, which may cause harms to organization.
Information Systems are also exposed to many direct and indirect risks. These risks primarily have emerged due to technological changes of information systems, these changes always create gap between protection applied and protection required, due to:

1. Widespread use of new technologies
2. Extensive use of network applications
3. Eliminations of distance, time and space constraints i.e. use of distributed or any time anywhere processing systems
4. Frequent technological changes
5. Attractiveness of conducting electronic attacks against organizations (electronic attacks are easy to conduct and hard to detect)

6. Devolutions or decentralization of management and control
7. Some external factors such as legal and regulatory requirements

The above gaps indicate that there are always emerging new risks areas that could have significant impacts on critical business operations such as:

(a) External dangers from hackers, leading to denial of service and virus attack, extortion and leakage of corporate confidential information
(b) Growing potential for misuse and abuse of information system affecting privacy and ethical values
(c) Dangers to information system availability and robustness

Question-20:

Information Systems Audit Report contains various components: Cover and title page, Table of Contents, Summary/Executive Summary and Appendices. But after submission, the principal auditor raised the query that the report is not correct as it missed various important components. Explain the missing components in brief.

Answer-20:

IS audit report is an end product of information system audit, conducted by an IS auditor. This report is communicated to management with auditor's opinions. Though there is no standard format or guidelines for preparation of this report, but overall this report may contain the followings:

- Cover and Title Page
- Table of Contents
- Executive Summary
- Introduction
    - Background of IT Environment or Context
    - Purpose of Audit
    - Scope of Audit
    - Methodology Used for Auditing
- Findings
- Opinions
- Appendices

If we look at all the components of an audit report from the above list then the major components missing from the submitted audit report are:

- **Introduction:** This section describes briefly about IT environment in which audit was conducted, purpose of audit, scope of audit and methods used for auditing.
- **Findings:** This includes the key findings from the concluded audits on the client system
- **Opinions:** This includes auditor's opinions about the client's information system in terms of adequacy of controls and information security etc
- **Appendices:** It includes various references which helped in an effective audit of client system during the audit assignment

Question-21:

An Information System Audit Report includes various sections: Title page, Table of Contents, Summary, Introduction, Findings and Appendices. Explain various elements, included in the Introduction section.

Answer-21:

Introduction is the key section of an audit report. It describes briefly about IT environment of client's organization, purpose of audit, scope of audit and methods used for auditing.

Since readers will read "Executive Summary" section before the introduction therefore "Introduction" section should not repeat details of "Executive Summary". It includes the following elements:

- **Context or Environment:** This sub-section briefly describes about the IT environment of client's organization. This sub-section also describes size/type of information system (speed, memory capacity, network structure etc) workload on information system and changes in the program and results of previous audits, etc.

- **Purpose:** This sub-section is a short description of what components, functions and special programs were audited.

- **Scope:** The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site audit dates.

- **Methodology:** This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client to make informed decisions as a result of audit report.