FINAL COURSE: GROUP – II
PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT
Question No. 1 is compulsory.
Attempt any five questions from the remaining six Questions.
Time Allowed – 3 Hours Maximum Marks – 100

Q-1) XYZ Industries Ltd. is a company engaged in the business of manufacturing and supplying of electronic equipments. It intends to implement E-Governance system at all of its departments. A system analyst is engaged to conduct requirements analysis and investigation of the present system. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate and reliable. The company is relying on Information Technology for information and transaction processing. It is also presumed that the company is up and running all the time on 24 x 7 basis. Hence, the company has decided to implement
a real time ERP package, which equips the enterprise with necessary capabilities to integrate and synchronize the isolated functions into streamlined business processes in order to gain a competitive edge in the volatile business environment. In addition, the company intends to keep all the records in digitized form. Read the above carefully and answer the following:

a) Explain the contents of System Requirement specification ?
b) What are the business risks that an organization may face while migrating to real time integrated ERP system?
c) What are the points that need to be taken into account for the proper implementation of physical and environmental security in respect of Information System Security?
d) What is the provision given in Information Technology (Amended) Act 2008 for the Sec 10 ?

Q-2)

1) Explain Design principles with modularity in SDLC? (6)
2) Explain preventive control with examples? Also describe characteristics of preventive control? (6)
3) Explain administrative safeguards of HIPAA? (4)

Q-3)

1) In Review of hard work, what are areas to be check in hardware acquisition plan? (6)
2) Roles Of IS auditor in Physical Access control ? (6)
3) Most qualitative risk analysis methodologies make use of a number of interrelated elements: explain those elements ? (4)

Q-4)

1) Explain Various alternate Processing Facilities? also explain reciprocal agreement (6)
2) Explain provisions of Secure E-signature and secure E-record? (6)
3) Explain various parts of Introduction section in IS audit Report? (4)

Q-5)

1) Explain the various Documents to be included in Disaster Recovery plan? (6)
2) Define Risk Mitigation ? and what are Risk mitigation measures? (6)
3) Explain CIS? (4)

Q-6)

1) What other factor should be considered for Evolution of Various ERP Packages? (6)
2) Explain various Testing Plan for testing BCP? (6)
3) Explain plan phase activities in ISO27001? (4)

Q-7) short notes (any four) (16)

1) Sec 41
2) Permanent file
3) Big bang and phased implementation
4) System maintenance
5) General model of system

ANS:
Q-1
(a)

A SRS contains the following:

- Introduction: Goals and Objectives of the software development
- Information Description: Like problem description; contents of Information, structure of Hardware, software; human interfaces for external system; etc.
- Functional Description: Diagrammatic representation of functions; processing of each function; interplay among functions; etc.
- Behavioral Description: Response to external events and internal controls
- Validation Criteria: Class of test to be performed to validate functions.
- Appendix: Data flow / Object Diagrams; Tabular Data; Detailed description of charts, graphs; etc.
- SRS Review: The development team makes a presentation and hands over the SRS document to management who reviews the same and if satisfied then signs the document.

(b)

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.

- Structural changes: Significant personnel and organizational structures changes associates with reengineering or redesigning business processes.

- Job role changes: Changes from traditional user's roles to empowered-based roles with much greater access to enterprise information in real time.

- Change management: It is a challenge to incorporate integrated environment when different business processes existed for so long. The level of user acceptance has a significant influence on the success of system. Training must therefore be provided to large number of users.

- Broad system access: Increased remote access by users due to integration among process allows increased access to application and data.

- Program interfaces and data conversions: Extensive interfaces and data conversions from old systems are 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. Due to relative complexity of ERP systems each specialist may know only a relatively small fraction of the entire ERP's functionality

- Data content quality: As enterprise applications are opened to external suppliers and customers, the need for data integrity becomes important.

(c)

For the proper implementation of Physical and Environment Security, the following points need to taken into account:

- Physical security should be maintained and checks must be performed to identify all vulnerable areas.
- The IT infrastructure must be physically protected.
- Access to secure areas must be to authorized staff only.
- Confidential and sensitive information and valuable assets must always be locked securely when not in use.
- Computers must never be left unattended whilst displaying confidential or sensitive information.
- Equipment, information or software must not be taken off-site without proper authorization.
- The location of the equipment room(s) must not be obvious. If practical should be located away from and protected against threats of unauthorized access and deliberate or accidental damage

(d)

Section 10: Power to make rules by Central Government in respect of Electronic Signature: The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of Electronic Signature;

(b) the manner and format in which the Electronic Signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the Electronic Signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to Electronic Signature.

Q-2)
(a)

Design Principles: [SMART]

- The design should be as per laid down standards.
- The design should be modular.
- The design should be based after analysis.
- The design should be related to business activities.
- There is a tendency to develop only one design and consider it as final. However it is recommended to develop two or three design and selects the best out of them.

  Modularity: A module is a manageable unit containing data and instructions to be performed in well-defined task. Interaction among modules is based on well-defined interfaces. Modularity is measured by two parameters: Cohesion and Coupling. Cohesion means the manner in which elements within a module are linked. Coupling refers to interconnection between the modules. In a good modular design, cohesion will be high and coupling low.

(b) Preventive Controls: Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act. The broad characteristics of preventive controls are:

(i) Understanding vulnerabilities of the asset
(ii) Understanding probable threats to the asset
(iii) Provision of necessary controls against materialization of probable threats

Examples of preventive controls

- Segregation of duties
- Access control
- Authorization of transaction
- Firewalls
- Anti-virus software (sometimes this acts like a corrective control also), etc
- Passwords

(c)
Administrative Safeguards: Administrative safeguards means policies and procedures are designed to clearly show how entity will comply with the act

- Covered entities (entities that must comply with HIPAA requirements) must follow a written set of privacy procedures and designate an officer to develop and implement all required policies and procedures.
- Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI).
- The procedures must address access through authorization only.
- Covered entities that out-source some of their business processes must ensure that their vendors also comply with HIPAA requirements.
- A contingency plan should be in place in case of emergencies.
- Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying security violations.
- There should be proper procedures to document cases of security breaches incident either during the audit or the normal course of operations.

Q-3)

(a)
Review the hardware acquisition plan to determine:

- Whether the IS management has issued written statements for acquisition of hardware.
- Whether the criteria for the acquisition of hardware are laid out.
- Whether the hardware acquisition plan is as per the strategic business plan of management.
- Whether there is awareness of the budget constraints.
- Whether all hardware are purchased after taking advantage of volume discounts or other quality benefits.
- Whether there is adequate space to accommodate the current and new hardware.
- Whether proper documentation has been maintained in respect of for hardware and software specifications, warranties, guarantees and likely lead-time associated with planned acquisitions.

(b)

This involves the following: [CPT is Risky]
Risk assessment: The auditor must satisfy himself that the risk assessment procedure adequately covers assessment of all assets, physical access threats, etc.
Controls assessment: The auditor must evaluate the physical access controls in place and whether they are adequate to protect the assets.
Planning for review of physical access controls: It requires examination of documentation like security policy and procedures, premises plans, building plans, inventory list, etc
Testing of controls: The auditor should review physical access controls to satisfy for their effectiveness. This involves:

- Physical inventory of computing equipment and supporting infrastructure.
- Interviewing personnel can also provide information on the awareness and knowledge of procedures.
- Inspection of :
  - ✓ Core computing facilities
  - ✓ Computer storage rooms
  - ✓ Communication closets
  - ✓ Backup and off site facilities
  - ✓ Printer rooms
  - ✓ Disposal yards and bins
  - ✓ Inventory of supplies and consumables

(c)
Most qualitative risk analysis methodologies make use of a number of interrelated elements:

- Threats: These are things that can go wrong or that can 'attack' the system. Eg: fire or fraud. Threats are ever present for every system.
- Vulnerabilities: These make a system more prone to attack by a threat or make an attack more successful or impactful. For example, for fire, vulnerability would be the presence of inflammable materials (e.g. paper).
- Controls: These are the countermeasures for vulnerabilities. There are four types: [what are the 4 counter measured for vulnerabilities?]
  - ✓ Deterrent controls reduce the likelihood of a deliberate attack

- ✓ Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
- ✓ Corrective controls reduce the effect of an attack
- ✓ Detective controls discover attacks and trigger preventative or corrective controls.

Q-4)
(a)

ALTERNATE PROCESSING FACILITY ARRANGEMENTS
Cold site: If an organization can tolerate some downtime (i.e., some downtime is available for recovery) then cold-site backup might be appropriate. Here, organization requires minimum facilities at an alternative location to run its regular operation like raised floors, air conditioning, power, communication lines, and so on. An organization can establish its own cold-site facility or enter into an agreement with another organization to provide a cold-site facility.

2. Hot site: If fast recovery is critical i.e., no downtime is tolerable, an organization might need hot site backup. Here, organization requires all the facilities at an alternative location. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organizations that have hot-site needs.

3. Warm site: A warm site provides an intermediate level of backup. Organization can tolerate some downtime. Here, organization requires only essential facilities at an alternative location. It has all cold-site facilities plus hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

4. Reciprocal agreement: Two or more organizations might agree to provide backup facilities to each other in the event of one suffering a disaster. This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.

(b)

SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES

Section 14: Secure Electronic Record: Section 14 provides where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification
.
Section 15: Secure Electronic Signature: Section 15 provides that an electronic signature shall be deemed to be a secure electronic signature if-
(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Section 16: Security procedures and Practices: The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices

(c)
It should include the following elements:

- ✓ Context: This sub-section briefly describes conditions prevailing in the audit entity during the period under audit, for instance, the entity's role, size and organization especially with regard to information system management, etc.

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

- ✓ Scope: The scope lists the period under review, the issues covered, the locations visited, etc.
- ✓ Methodology: This section briefly describes sampling, data collection techniques and the basis for auditors' opinions.

Q-5)

(a)

The disaster recovery and planning document may include the following areas:

- The conditions for activating the plans describing the process to be followed before activation.
- Emergency procedures, which describe the actions to be taken following an incident (ie., disaster) which jeopardizes business operations and/or human life which include effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- Fallback procedures i.e., condition to be satisfied to move essential business activities to alternate temporary locations.
- Resumption procedures, which describe the actions to be taken to return to normal business operations.
- A schedule for testing and for maintaining the plan.
- The responsibilities of individuals describing who is responsible for executing the plan. Alternatives should be nominated as required.
- Contingency plan should be kept ready.
- Detailed description of the purpose and scope of the plan.
- List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- List of phone numbers of employees in the event of an emergency.
- Emergency phone list of fire, police, hardware, software, suppliers, customers, back-up location, etc
- Medical procedure to be followed in case of injury.
- Back-up location contractual agreement, correspondences.
- Insurance papers and claim forms.

- Names of employees trained for emergency situation, first aid and life saving techniques.
- Details of airlines, hotels and transport arrangements.

(b)

RISK MITIGATION: An analysis helps to relate characteristics of an event to the probability and severity of the operational losses. This will enable the organization to decide whether or not to invest in information system or people so that events or the effect of events can be minimized. A causal understanding is required to manage and control risks. Knowing 'what causes what' will give an understanding of risk and helps to implement the necessary controls.

Risk mitigation Measures:

- Self assessment
- Strong internal control
- Developing operational risk department
- Crete Disaster Recovery Plan
- Insurance
- Outsourcing

(c)

Continuous and Intermittent Simulation (CIS): This is a variation of a SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:

- The database management system reads the transaction which is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the database management system.
- CIS replicates or simulates the application system processing.
- CIS then checks this processed transaction to determine whether any discrepancies exist between the results it produces and those the application system produces.
- Exceptions identified by CIS are written on to exception log file.
- The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

Q-6)

(a)

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.

(b)

There are four types of tests:

1. Hypothetical: It verifies the existence of all necessary procedures and actions within the recovery plan. It is a theoretical check.

2. Component: A component is the smallest set of instructions to be performed by processes within the recovery plan. Component testing is designed to verify the detail and accuracy of individual procedures within the recovery plan

3. Module: A module is a combination of components. The ideal method of module testing is that each component be individually tested before being included in a module. The aim of module testing is to verify the functionality of the recovery procedures when multiple components are combined.

4. Full: The full test verifies whether each component within every module is workable and satisfies the strategy and recovery time specified in the recovery plan

(c)

The Plan phase:

The Plan phase consists of the following steps:

- Determining the scope of the ISMS;
- Writing an ISMS Policy;
- Identifying the methodology for risk assessment and determining the criteria for risk acceptance;
- Identification of assets, vulnerabilities and threats;
- Evaluating the size of risks;
- Selection of controls for risk treatment;
- Obtaining management approval for residual risks;and
- Obtaining management approval for implementation of the ISMS;

Q-7)

(a)

Section 41: Acceptance of Digital Signature Certificate:

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes Digital Signature Certificate -

(a) To one or more persons;

(b) Demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber and information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate is true which is within the knowledge of the subscriber.

(b)

The permanent audit file normally includes:

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

(c)

“Big Bang” or Phased Implementation?

- A “big bang” implementation involves implementing all modules at all locations at the same time. Characteristics of this approach include no need for temporary interfaces, cross-module functionality and overall cost, if no contingencies arise.
- Phased implementation includes implementation of one or a group at a time often a single location at a time.

Benefits of this approach include: a smoothing of resource requirements, an ability to focus on a particular module, availability of existing systems incase of fall-back, reduced risk, the knowledge gained with each phase and the usefulness of demonstrable working system.

(d)

Maintaining the system is an important aspect of SDLC. Maintenance can be categorized in the following ways:

- Scheduled maintenance: Scheduled maintenance is anticipated and can be planned for. For eg., the implementation of a new inventory coding scheme can be planned in advance.
- Rescue maintenance: Rescue maintenance refers to previously undetected errors that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.

    - Corrective maintenance: Corrective maintenance deals with fixing bugs (i.e., fixing solution) in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors.
    - Adaptive maintenance: Adaptive maintenance consists of adapting software as per changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions from outside the on the system, for example, business rule, government policies, etc.
- Perfective maintenance: Perfective maintenance mainly deals with accommodating to new or changed user requirements and activities to increase the system's performance or to enhance its user interface.
- Preventive maintenance: Preventive maintenance activities aim at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system

(e)

A General model of System :

- Input is the data flowing into the system from outside. For example: A newspaper takes a news feed from a news wire service such as Reunters.
- Processing is the action of manipulating the input into a more useful from. For example : The newspaper takes the pure text obtained from the news wire service and creates front page layout using pictures and formatted text.
- Output is the information flowing out of a system. For example : The raw news wire information is viewed on your website as a story, all nicely formatted in the company style.

- Storage is the means of holding information for use at a later date.
- Feedback occurs when the outcome has an influence on the input.