

MOCK TEST PAPER – 2
FINAL COURSE: GROUP – II
PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT
SUGGESTED ANSWERS/HINTS

1. (a) **Enterprise Resource Planning (ERP) Systems** : ERP is one of the latest high-end solutions that seek to streamline and integrate operation processes and information flows in the company to synergize the five major resources of an organization namely men, money, machine, material and market. Formally, ERP can be defined as follows:

“An ERP system is a fully integrated business management system that integrates the core business and management processes to provide an organization a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable real-time information.”

- (b) Yes, we agree with the decision of the management. Major points for supporting their decision are given as follows:
- It provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.
 - It supports strategic and business planning activities, operational planning and execution activities etc. All these functions are effectively integrated for flow and update of information immediately upon the entry of any information.
 - It facilitates company-wide Integrated Information System, covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory, accounts, human resources, purchases etc.
 - It provides complete integration of systems not only across departments but also across companies under the same management.
 - It is the solution for better project management.
 - It allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Internet, Intranet, Video conferencing, E-Commerce etc.
 - It eliminates most of the business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.
 - It provides intelligent business tools like decision support system, Executive information system, Data mining and easy working systems to enable better decisions.

- (c) ERP implementation also engenders a host of fears. Some of these fears are given as under:
- Job redundancy;
 - Loss of importance as information is no longer an individual prerogative;
 - Change in job profile;
 - An organizational fear of loss of proper control and authorization;
 - Increased stress caused by greater transparency; and
 - Individual fear of 'loss of authority'.
- (d) The business risks that ABC India Ltd. can face while migrating to real time integrated ERP system are given as follows:
- Single point of failure: Since entire organization's data and transaction processing is within one application system; single point failure may be a major risk.
 - Structural changes: Significant personnel and organizational structure changes associated with reengineering or redesigning business processes may pose a big challenge.
 - Job role changes: Transition of traditional user's roles to empowered-based roles with much greater access to enterprise information in real time and the point of control shifting from the back-end financial processes to the front-end point of creation are also great risks.
 - Online, real-time: An online real-time environment requires a continuous business environment capable of utilizing the new capabilities of the ERP application and responding quickly to any problem requiring re-entry of information.
 - Change management: The level of user acceptance of the system has a significant influence on its success. Users must understand that their actions or inaction may have a direct impact on the other users and, therefore, they must learn to be more diligent and efficient in the performance of their day-to-day duties.
 - Distributed computing experience: Inexperience with implementing and managing distributed computing technology may pose significant challenges.
 - Broad system access: Increased remote access by users and outsiders and high integration among application functions allow increased access to application and data.
 - Dependency on external assistance: Organization accustomed to in-house legacy systems may find that they have to rely on external help. Unless such

external assistance is properly managed, it could introduce an element of security and resource management risk that may expose the organizations to greater risk.

- Program interfaces and data conversions: Extensive interfaces and data conversions from legacy systems and other commercial software are often necessary. The exposure of data integrity, security and capacity requirements for ERP are therefore often much higher.
- Audit expertise: Specialist expertise is required to effectively audit and control an ERP environment. The relative complexity of ERP systems has created specialization such that each specialist may know a small fraction of the entire ERP's functionality in a particular core module.

2. (a) Major boundary control techniques are given as follows:

- Cryptography: It deals with programs for transforming data into codes that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution)
- Passwords: User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices, followed to avoid failures in this control system are: minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.
- Personal Identification Numbers (PIN): The personal identification number is similar to a password assigned to a user by an institution based on the user characteristics and encrypted using a cryptographic algorithm, or the institute generates a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN or a digital signature are exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- Identification Cards: Identification cards are used to store information required in an authentication process. These cards used to identify a user, are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.

(b) The effectiveness and efficiency of the system maintenance process is evaluated with the following metrics:

- The ratio of actual maintenance cost per application/operation v/s the average of all applications/process;
- Average time to deliver change requests;
- The number of change requests for the system application that were related to bugs, critical errors, and new functional specifications;
- The number of production problems per application and per respective maintenance changes;
- The instances of divergence from standard procedures such as undocumented applications, unapproved design, and testing reductions;
- The quantity of modules returned to development due to errors discovered in acceptance testing; and
- Time elapsed to analyze and fix problems.

(c) [Section 30] Duties of Certifying Authorities:

This section provides that every Certifying Authority shall follow certain procedures in respect of Digital Signatures as given below: Every Certifying Authority shall-

- (a) make use of hardware, software, and procedures that are secure from intrusion and misuse;
- (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- (c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured (Amended vide ITAA 2008)
 - (ca) be the repository of all Electronic Signature Certificates issued under this Act (Inserted vide ITAA 2008)
 - (cb) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and (Inserted vide ITAA 2008)
- (d) observe such other standards as may be specified by regulations.

3. (a) As given in the scenario, XYZ Ltd. is primarily engaged in games development and after considering all the relevant factors, the technical consultant of the company recommended to follow a combination of prototyping and waterfall model for the project implementation, the model to be used would be Spiral.

The spiral model is a software development process, combining elements of both design and prototyping-in-stages, in an effort to combine the 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 both. The spiral model is intended for large, expensive and complicated projects. 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.

Its basic principles are given as follows:

- The new system requirements are defined in details as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.
 - A preliminary design is created for the new system. This phase is the most important part of 'Spiral Model'; in which all the 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.
 - 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.
 - A second prototype is evolved through a fourfold procedure by:
 - ◆ 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.
- (b) A permanent audit file normally includes the following:
- The organizational 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) Major weaknesses associated with packet filtering firewalls are given as follows:

- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents.
- Logging functionality is limited to the same information used to make access control decisions.
- Most of these firewalls do not support advanced user authentication schemes.
- Firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
- The firewalls are easy to mis-configure, which allows traffic to pass that should be blocked.

4. (a) Risk Assessment: Risk assessment is a step in the risk management procedure. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat. A risk assessment can provide an effective approach that will serve as the foundation for avoiding of disasters. Through risk analysis, it is possible to identify, assess and then mitigate the risk.

Risk Assessment is a critical step in disaster and business continuity planning. Risk Assessment is the analysis of 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 in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan.

The areas to be focused upon are given as follows:

- (i) Prioritization: All applications are inventoried and critical ones identified. Each of the critical application is reviewed to access its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.
- (ii) Identifying critical applications: Amongst the applications, currently being processed the critical applications are identified. Further analysis is done to determine specific jobs in the applications, which may be more critical. Even though the critical value would be determined based on its present value, future changes should not be ignored.
- (iii) Assessing their impact on the organization: Business Continuity Planning (BCP) should not concentrate only on business disruption but should also take into account other organizational functions, which may be affected. The areas to be considered include:
 - Legal liabilities,

- Interruptions of customer services,
 - Possible losses, and
 - Likelihood of fraud and recovery procedures.
- (iv) Determining recovery time-frame: Critical recovery time period is the period of time in which business processing must be resumed before the organization incurs severe losses. This critical time depends upon the nature of operations. It is essential to involve the end users in the identification of critical functions and critical recovery time period.
- (v) Assess Insurance Coverage: The information system insurance policy should be a multiperil 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:
- o 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.
 - o Software reconstruction: In addition to the cost of media, programming costs for recreating the software should also be covered.
 - o Extra expenses: The cost incurred for continuing the operations till the original facility is restored should also be covered.
 - o Business interruption: This applies mainly to centres performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.
 - o Valuable paper and records: The actual cost of valuable papers and records stored in the insured premises should be covered.
 - o Errors and omissions: This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmes and other information system personnel.
 - o Fidelity coverage: This coverage is for acts of employees in the case of financial institutions, which use their own computers for providing services to clients.
 - o Media transportation: The potential loss or damage to media while being transported to off-site storage / premises should be covered.
- (vi) Identification of exposures and implications: It is not possible to accurately predict as to when and how a disaster would occur. So, it is necessary to estimate the probability and frequency of disaster.
- (vii) Development of recovery plan: The plan should be designed to provide for recovery from total destruction of a site.

- (b) Various tasks, which are to be undertaken in 'Business Impact Analysis' phase are given as follows:
- Identify organisational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimise 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 organisation in the event of a disaster, e.g. financial reputation, etc.
- (c) Major design principles with reference to SDLC are described as follows:
- There is a tendency to develop merely one design and consider it the final product. However the recommended procedure is to design two or three alternatives and choose the best one on pre-specified criteria.
 - The design should be based on the analysis.
 - The software functions designed should be directly relevant to business activities.
 - The design should follow standards laid down. For instance, the user interface should have consistent color scheme, menu structure, location of error message and the like.
 - The design should be modular.
5. (a) Expert System: An Expert System is a highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem. Expert System is software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – how much can be invested. Does the client have any preferences regarding specific types of securities? And so on.

Some of the business applications of Expert Systems are given as follows:

- Accounting and Finance: It provides tax advice and assistance, helping with credit-authorization decisions, selecting forecasting models, providing investment advice.
 - Marketing: It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.
 - Manufacturing: It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and facility layouts.
 - Personnel: It is useful in assessing applicant qualifications, giving employees assisting at filling out forms
 - General Business: It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.
- (b) Detailed controls and objectives of 'Communications and Operations Management' with reference to Information Security Management System (ISMS) are given as follows:
- Operational procedures and responsibilities: To ensure correct and secure operation of information processing facility;
 - System planning and acceptance : To minimize risk of system failure;
 - Protection against malicious software: To protect the integrity of software and information;
 - Housekeeping: To maintain the integrity and availability of information processing and communication services;
 - Network Management: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
 - Media handling and security: Prevent damage to assets and interruptions to business activity; and
 - Exchanges of information and software: To prevent loss, modification or misuse of information exchanged between organizations.
- (c) Three levels of implementation of databases are given as follows:
- Physical level: It involves the implementation of the database on the hard disk i.e. storage of data in the hard disk. The management of storage and access is controlled by operating system.
 - Logical Level: It is designed by professional programs, who have the

complete knowledge of DBMS. It deals with the nature of data stored, the scheme of the data. Storage which is logically divided into various tables having rows and columns and the techniques for defining relationships with indexes.

- External level: The logical level defines schema, which is divided into smaller units known as sub-schemas and given to the managers each sub-schema containing all relevant data needed by one manager.
6. (a) Various tasks covered under the second phase of developing a business continuity plan i.e. 'Vulnerability Assessment and definition of requirement' are given as follows:
- A thorough Security Assessment of the system and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
 - The Security Assessment will enable the business continuity team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
 - Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
 - Define the scope of the planning effort.
 - Analyze, recommend and purchase recovery planning and maintenance software required to support the development and maintenance of the plans.
 - Develop a Plan Framework.
 - Assemble business continuity team and conduct awareness sessions.
- (b) Various Data Integrity Policies are given as follows:
- Virus-Signature Updating: Virus signatures must be updated immediately when they are made available from the vendor.
 - Software Testing: All software must be tested in a suitable test environment before installation on production systems.
 - Division of Environments: The division of environments into Development, Test, and Production is required for critical systems.
 - Version Zero Software: Version zero software (1.0, 2.0, and so on) must be

avoided whenever possible to avoid undiscovered bugs.

- Offsite Backup Storage: Backups older than one month must be sent offsite for permanent storage.
- Quarter-End and Year-End Backups: Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes.
- Disaster Recovery: A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

(c) During the review of hardware, review of the hardware acquisition plan is accomplished by the following:

- Whether the IS management has issued written policy statements regarding the acquisition of hardware;
- Whether the criteria for the acquisition of hardware are laid out and procedures and forms established to facilitate the acquisition approval process;
- Whether the hardware acquisition plan is in concurrence with the strategic business plan of management;
- Whether there is awareness of the budget constraints;
- Whether the requests for the acquisition of hardware are supported by cost benefit analysis;
- Whether all hardware are purchased through IS purchasing department to take advantage of volume discounts or other quality benefits;
- Whether the environment is conducive and space is adequate to accommodate the current and new hardware;
- Whether IS management's hardware acquisition plan has taken into consideration technological obsolescence of the installed equipment, as well the new equipment in the acquisition plan;
- Whether there has been a consideration of lease expirations on current equipment; and
- Whether documentation for hardware and software specifications, installation requirements, warranties, guarantees and likely lead-time associated with planned acquisitions is properly maintained.

7. (a) Time Bomb: This name has been borrowed from its physical counterpart because of the mechanism of the activation. A physical time bomb explodes at the time, it is set for (unless somebody forces it to explode early), like wise the computer time bomb causes a perverse activity, such as, disruption of computer system, modifications, or destructions of stored information etc. on a particular date and time for which it has been developed. The computer clock initiates it.

Logic Bomb: They resemble time bombs in their destruction activity. Logic bombs are activated by combination of events. For example, a code like; "If a file named DELETENOT is deleted then destroy the memory contents by writing ones." This code segment, on execution, may cause destruction of the contents of the memory on deleting a file named DELETENOT. These bombs can be set to go off at a future time or event.

- (b) Corrective maintenance: Corrective maintenance deals with fixing bugs in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.

Adaptive maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.

- (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.

- (d) "Big Bang" Implementation of ERP: A "big bang" implementation involves 'having all modules at all locations implemented at the same time'. Characteristics of this approach include:

- no need for temporary interfaces,
- limited requirement to maintain legacy software,
- cross-module functionality and
- overall cost if no contingencies arise.

Phased Implementation of ERP: Phased implementation means 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,
 - avail-ability of existing legacy systems as a fall-back,
 - reduced risk,
 - the knowledge gained with each phase and
 - the usefulness of demonstrable working system.
- (e) [Section 90] Power of State Government to make rules of Information Technology (Amended) Act, 2008:
- (1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.
 - (2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely
 - (a) the electronic form in which filing, issue, grant receipt or payment shall be effected under sub-section (1) of section 6;
 - (b) for matters specified in sub-section (2) of section 6;
 - (3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.