

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

1. (a) Some popular expectations from an ERP solution is given as follows:
- An improvement in processes;
 - Increased productivity on all fronts;
 - Total automation and disbanding of all manual processes;
 - Improvement of all key performance indicators;
 - Elimination of all manual record keeping;
 - Real time information systems available to concerned people on a need basis; and
 - Total integration of all operations.
- (b) The Change Control process of a system under development is to address the problems not detected during system design or testing and change in user requirements. A change control evaluation includes checks on problems reporting, tracking, prioritizing, and resolving, and if changes are authorized, tested, documented, and communicated through a legitimate management responsibility. The risks dealt with the change control processes are given as under:
- System outages due to error, omissions, or malicious intent,
 - Data loss or errors due to error, omissions, or malicious intent,
 - Unauthorized changes,
 - Fraud/abuse to company systems and/or data,
 - Repeated errors, and
 - Reruns of system or application processes.
- The objective of a change management review is to ensure that changes made to the system and programs do not adversely affect system, application, or data availability or integrity. Auditors need to verify that all changes made to the systems and programs are appropriately authorized and documented.
- (c) The controls and objectives of System Development and Maintenance are given as follows:
- *Security requirements of system:* To ensure that security is built into information systems;

- *Security in application systems*: To prevent loss, modification or misuse of user data in application system;
- *Cryptographic Controls*: To protect the confidentiality, authenticity or integrity of information;
- *Security of system files*: To ensure that IT projects and support activities are conducted in a secure manner; and
- *Security in development and support process*: To maintain the security of application system software and information.

(d) A security policy should cover the following major issues:

- a definition of information security,
- a statement of management intention supporting the goals and principles of information security,
- allocation of responsibilities for every aspect of implementation,
- an explanation of specific applicable proprietary and general, principles, standards and compliance requirements,
- an explanation of the process for reporting of suspected security incidents,
- a defined review process for maintaining the policy document,
- means for assessing the effectiveness of the policy embracing cost and technological changes, and
- nomination of the policy owner.

2. (a) Most common security threats are given as follows:

- Access to confidential data,
- Unauthorized access of the department computers,
- Password disclosure compromise,
- Virus infections,
- Denial of service attacks,
- Open ports, which may be accessed from outsiders, and
- Unrestricted modems unnecessarily open ports.

(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) [Section 41] Acceptance of Digital Signature Certificate:

- (1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate -
 - (a) to one or more persons;
 - (b) in a repository, or otherwise 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 to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
 - (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

3. (a) Major benefits of Expert Systems are given as follows:

- Expert Systems preserve knowledge that might be lost through retirement resignation or death of an acknowledged company expert.
- Expert Systems put information into an active-form so it can be summoned almost as a real-life expert might be summoned.
- Expert Systems assist novices in thinking the way experienced professional do.
- Expert Systems are not subject to such human fallings as fatigue, being too busy, or being emotional.
- Expert Systems can be effectively used as a strategic tool in the areas of marketing products, cutting costs and improving products.

(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: Protection 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 teleporting: To ensure information security when using mobile computing & teleworking facilities.*

(c) Some of the major weaknesses of Waterfall model are given as follows:

- Waterfall Model is Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- By adapting this model, project progresses forward, with only slight movement backward.
- It provides little room for use of iteration, which can reduce manageability if used.
- It depends upon early identification and specification of requirements, yet users may not be able to clearly define what they need early in the project.
- Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding, if we adapt this model.
- Problems are often not discovered until system testing, if we use waterfall approach.
- System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- It is difficult to respond to changes. Changes that occur later in the life cycle are more costly and are thus discouraged.
- It produces excessive documentation and keeping it updated as the project progresses is time-consuming.
- Written specifications are often difficult for users to read and thoroughly appreciate.
- Promotes the gap between users and developers with clear vision of responsibility.

4. (a) The **Delphi Technique** 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.

(b) 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 major 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.

These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

(c) While utilizing PKI policies and controls, financial institutions need to consider the following:

- Defining within the certificate issuance policy the methods of initial verification that are appropriate for different types of certificate applicants and the controls for issuing digital certificates and key pairs;
- Selecting an appropriate certificate validity period to minimize transactional and reputation risk exposure—expiration provides an opportunity to evaluate the continuing adequacy of key lengths and encryption algorithms, which can be changed as needed before issuing a new certificate;
- Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions accompanied by a certificate;
- Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a user's private key or the closing of user accounts;

- Updating the database of revoked certificates frequently, ideally in real-time mode;
- Employing stringent measures to protect the root key including limited physical access to CA facilities, tamper-resistant security modules, dual control over private keys and the process of signing certificates, as well as the storage of original and back-up keys on computers that do not connect with outside networks;
- Requiring regular independent audits to ensure controls are in place, public and private key lengths remain appropriate, cryptographic modules conform to industry standards, and procedures are followed to safeguard the CA system;
- Recording in a secure audit log all significant events performed by the CA system, including the use of the root key, where each entry is time/date stamped and signed;
- Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions and unauthorized activities; and
- Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require the acceptance of the financial institution's certificates by other CAs.

5. (a) Four important benefits of Office Automation Systems are given as follows:

- Office Automation Systems improve communication within an organization and between organizations.
- Office Automation Systems reduce the cycle time between preparation of messages and receipt of messages at the recipients' end.
- Office Automation Systems reduce the costs of office communication both in terms of time spent by executives and cost of communication links.
- Office Automation Systems ensure accuracy of communication flows.

(b) A few common threats to the computerized environment can be:

- **Power failure:** Power failure can cause disruption of entire computing equipments since computing equipments depends on power supply.
- **Communication failure:** Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where the organization depends on public communication lines e.g. for e-banking, communication failure present a significant threat that will have a direct impact on operations.
- **Disgruntled Employees:** A disgruntled employee presents a threat since, with

access to sensitive information of the organization, he may cause intentional harm to the information processing facilities or sabotage operations.

- **Errors:** Errors which may result from technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the firewall to “allow” attachments instead of “deny” may result in the entire organization network being compromised with virus attacks.
 - **Malicious Code:** Malicious code such as viruses and worms which freely access the unprotected networks may affect organizational and business networks that use these unprotected networks.
 - **Abuse of access privileges by employees:** The security policy of the company authorizes employees based on their job responsibilities to access and execute select functions in critical applications.
 - **Natural disasters:** Natural disasters such as earthquakes, lighting, floods, tornado, tsunami, etc. can adversely affect the functioning of the Information System operations due to damage to Information System facilities.
 - **Theft or destruction of computing resources:** Since the computing equipments form the back-bone of information processing, any theft or destruction of the resource can result in compromising the competitive advantage of the organization.
 - **Downtime due to technology failure:** Information System facilities may become unavailable due to technical glitches or equipment failure and hence the computing infrastructure may not be available for short or extended periods of time. However, the period for which the facilities are not available may vary in criticality depending on the nature of business and the critical business process that the technology supports.
 - **Fire, etc. :** Fire due to electric short circuit or due to riots, war or such other reasons can cause irreversible damage to the IS infrastructure.
- (c) **Unit Testing:** In computer programming, unit testing is a software verification and validation method in which a programmer tests if individual units of source code are fit for use. A unit is the smallest testable part of an application which may be an individual program, function, procedure, etc. or may belong to a base/super class, abstract class or derived/child class.

Unit tests are typically written and run by software developers to ensure that code meets its design and behaves as intended. The goal of unit testing is to isolate each part of the program and show that the individual parts are correct. A unit test provides a strict, written contract that the piece of code must satisfy.

There are five categories of tests that a programmer typically performs on a program unit:

- **Functional Tests:** Functional Tests check 'whether programs do what they are supposed to do or not'. The test plan specifies operating conditions, input values, and expected results, and as per this plan programmer checks by inputting the values to see whether the actual result and expected result match.
- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
- **Stress Tests:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. For example, during a sort operation, the available memory can be reduced to find out whether the program is able to handle the situation.
- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

6. (a) [Section 19] Recognition of foreign Certifying Authorities :

- (1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.
- (2) Where any Certifying Authority is recognized under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
- (3) The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under subsection (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

- (b) Application-Level Firewalls:** Application-level firewalls 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. Unlike a packet filter firewall, an application-level firewall continues to

examine 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. Application level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.

The primary disadvantages of application-level firewalls are as follows:

- The time required to read and interpret each packet slows network traffic. Traffic of certain types may have to be split off before the application-level firewall and passed through different access controls.
- Any particular firewall may provide only limited support for new network applications and protocols. They also simply may allow traffic from those applications and protocols to go through the firewall.

(c) 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.

7. (a) **TPS Components** : The principal components of a TPS include inputs, processing, storage and outputs. These are given as follows:

- **Inputs**: Source documents, such as customer orders, sales, slips, invoices, purchase orders, and employee time cards, are the physical evidence of inputs into the Transaction Processing System. They serve several purposes like - capturing data, facilitating operations by communicating data and authorizing another operation in the process, standardizing operations by indicating which data require recording and what actions need to be taken, and providing a permanent file for future analysis, if the documents are retained etc.
- **Processing**: This involves the use of journals and registers to provide a

permanent and chronological record of inputs. Journals are used to record financial accounting transactions, and registers are used to record other types of data not directly related to accounting. Some of the more common special journals are – sales journal, purchase journal, cash receipts journal etc.

- **Storage:** Ledgers and files provide storage of data on both manual and computerized systems. The general ledger, the accounts/vouchers payable ledgers, and the accounts receivable ledger are the records of final account that provide summaries of a firm's financial accounting transactions.
- **Outputs:** Any document generated in the system is output. Some documents are both output and input. For example - a customer invoice is an output from the order-entry application system and also an input document to the customer. The trial balance lists the balances of all the accounts on the general ledger and tests the accuracy of the record keeping. Financial reports summarize the results of transaction processing and express these results in accordance with the principles of financial reporting.

(b) Operational Feasibility: It is concerned with ascertaining the views of workers, employees, customers and suppliers about the use of computer facility. A system can be highly feasible in all respects except the operational and fails miserably because of human problems. Some of the questions which help in testing the operational feasibility of a project are stated below:

- Is there sufficient support for the system from management and from users?
- Are current business methods acceptable to users?
- Have the users been involved in planning and development of the project?
- Will the proposed system cause harm? Will it produce poorer results in any respect or area? Will loss of control result in any areas? Will accessibility of information be lost?
- Will individual performance be poorer after implementation than before?

This analysis may involve a subjective assessment of the political and managerial environment in which the system will be implemented. In general, the greater the requirements for change in the user environment in which the system will be installed, the greater the risk of implementation failure.

(c) Preventive maintenance: Preventive maintenance concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

Perfective maintenance: **Perfective maintenance** mainly deals with accommodating to new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.

(d) Role of an IS auditor in evaluating logical access controls: An IS auditor should keep the following points in mind while working with logical access control mechanisms:

- Reviewing the relevant documents pertaining to 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.

(e) Major advantages of continuous audit techniques are given as under:

- *Timely, comprehensive and detailed auditing* – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
- *Surprise test capability* – As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- *Information to system staff on meeting of objectives* - Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- *Training for new users* – Using the ITFs new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.