

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

1. (a) System requirements analysis is a phase, which includes a thorough and detailed understanding of the current system, identification of the areas that need modification/s to solve the problem, the determination of user/managerial requirements and to have fair ideas about various system development tools.

The following major activities are performed in this phase:

- To identify and consult the stake owners to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine priorities;
- To verify requirements in terms of various parameters like completeness, consistency, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like- interviewing, research/document collection, questionnaires, observation;
- To develop models to document Data Flow Diagrams, E-R diagrams; and
- To document activities such as interviews, questionnaires, reports etc. and development of a system dictionary to document the modeling activities.
- The document/deliverable of this phase is a detailed system requirements report, which is generally termed as SRS.

- (b) Organizations face several business risks when migrating to real-time, integrated ERP systems. These risks are given as follows:

- *Single point of failure:* Since all the 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 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.
 - *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.
- (c) For the proper implementation of Physical and Environmental Security, the following points need to be taken into account:
- Physical security should be maintained and checks must be performed to identify all vulnerable areas within each site.
 - The IT infrastructure must be physically protected.
 - Access to secure areas must remain limited to authorized staff only.
 - Confidential and sensitive information and valuable assets must be securely locked away, when they are not in use.
 - Computers must never be left unattended whilst displaying confidential or sensitive information or whilst logged on to the systems.

- Supplies and equipments must be delivered and loaded in an isolated area to prevent any unauthorized access to key facilities.
- Equipment, information or software must not be taken off-site without proper authorization.
- Wherever practical, premises housing computer equipment and data should be located away from, and protected against threats of deliberate or accidental damage such as fire and natural disaster.
- The location of the equipment rooms must be away from, and protected against threats of unauthorized access and deliberate or accidental damage, such as system infiltration and environmental failures.

(d) Retention of Electronic Records: [Section 7] of ITAA 2008 : The provision for the retention of electronic records is discussed in Section 7 of ITAA 2008, which is given as follows:

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

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.

2. **(a)** In case of acquisition of a software system, the following controls need to be in place:
 - Information and system requirements need to meet business and system goals, system processes to be accomplished, and the deliverables and

expectations for the system. The techniques are interviews, deriving requirements from existing systems, identifying characteristics from related system, and discovering them from a prototype or pilot system.

- A feasibility analysis to define the constraints or limitations for each alternative system from a technical as well as a business perspective. It should also include economic, technical, operational, schedule, legal or contractual, and political feasibility of the system within the organization scope.
 - A detailed Request for Proposal (RFP) document needs to specify the acceptable requirements (functional, technical, and contractual) as well as the evaluation criteria used in the vendor selection process. The selection criteria should prevent any misunderstanding or misinterpretation.
 - While identifying various alternatives software acquisition involves the critical task of vendor evaluation. The vendor evaluation process considers the following:
 - ◆ Stability of the supplier company,
 - ◆ Volatility of system upgrades,
 - ◆ Existing customer base,
 - ◆ Supplier's ability to provide support,
 - ◆ Cost-benefits of the hardware/software in support of the supplier application, and
 - ◆ Customized modifications of the application software.
- (b) The detailed controls and objectives of System Development and Maintenance under ISMS 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.

(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.

3. (a) Four 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) Following points are required to be taken into consideration for access control relating to Information Security Policy:

- Access controls must be in place to prevent unauthorized access to information systems and computer applications
- Access must be granted only in response to a business requirement. Formal processes must be in place to provide individuals with access. The requirement for access must be reviewed regularly.
- System Owners are responsible for approving access to systems and they must maintain records of who has access to a particular system and at what level. The actual access controls in place must be audited against this record on a regular basis.

- Users should be granted access to systems only up to the level required to perform their normal business functions.
 - The registration and de-registration of users must be formally managed.
 - Access rights must be deleted for individuals who leave or change jobs.
 - Each individual user of an information system or computer application will be provided with a unique user identifier (user id)
 - It should not be permitted for an individual to use another person's user id or to log-on, to allow another individual to gain access to an information system or computer application.
 - PCs and terminals should never be left unattended whilst they are connected to applications or the network. Someone may use the equipment to access confidential information or make unauthorized changes.
 - Passwords Policy should be defined and the structure of passwords and the duration of the passwords should be specified. Passwords must be kept confidential and never disclosed to others.
 - Mobile computing - When using mobile computing facilities, such as laptops, notebooks, etc., special care should be taken to ensure that business information is not compromised, particularly when the equipment is used in public places.
- (c) **Adaptive Maintenance:** It 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.

Preventive Maintenance: It concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. 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.

4. (a) Four major categories under which various strategies are made to manage the risk are given as follows:
- **Risk Avoidance:** It means 'not doing an activity that involves risk'. It involves losing out on the potential gain that accepting the risk might have provided, e.g. not using Internet / public network on a system connected to

organization's internal network, instead using a stand-alone PC for Internet usage.

- **Risk Mitigation/Reduction:** It involves implementing controls to protect IT infrastructure and to reduce the severity of the loss or the likelihood of the loss from occurring; e.g. using an effective anti-virus solution to protect against the risk of viruses and updating it on timely basis.
- **Risk Transfer:** It involves causing another party to accept the risk i.e. sharing risk with partners or insurance coverage.
- **Risk Retention/Acceptance:** It means formally acknowledging that the risk exists and monitoring it. In some cases it may not be possible to take immediate action to avoid/mitigate the risk. All risks that are not identified or avoided or transferred are retained by default. These risks are called residual risks. Risk management aims to identify, select and implement the controls that are necessary to reduce residual exposures to acceptable levels.

The goals and mission of an organization should be considered in selecting any of these risk management strategies. It may not be practical to address all identified risks, so priority should be given to the risks that have the potential to cause significant mission impact or harm.

- (b) *Incremental Backup:* An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.

Normally, incremental backup are very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

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.

- (c) Major weaknesses of Waterfall Model is given as follows:
- Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.

- Project progresses forward, with only slight movement backward.
 - Little room for use of iteration, which can reduce manageability if used.
 - 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.
 - Problems are often not discovered until system testing.
 - System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
 - Difficult to respond to changes. Changes that occur later in the life cycle are more costly and are thus discouraged.
 - 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.
5. (a) The metrics, which help in the evaluation of effectiveness and efficiency of the system maintenance process are given as follows:
- The ratio of actual maintenance cost per application/operation versus 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.
- (b) **Acquire and Implement:** The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT

system and its components. The following table lists the IT processes contained in the Acquire and Implement domain.

IT PROCESSES
Acquire and Implement

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredited Solutions and Changes

- (c) **Information:** Information is the data that have been put into a meaningful and useful context. It has been defined by Davis and Olson as - "Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision". For example, data regarding sales by various salesmen can be merged to provide information regarding total sales through sales personnel. This information is of vital importance to a marketing manager who is trying to plan for future sales.

Some of the important attributes of useful and effective information are given as follows:

- (i) **Availability:** Availability or Timeliness is a very important property of information. If information is not available at the time of need, it is useless. Data is organized in the form of facts and figures in databases and files from where various information is derived for useful purpose.
- (ii) **Purpose:** Information must have purposes at the time it is transmitted to a person or machine, otherwise it is simple data. Information communicated to people has a variety of purposes because of the variety of activities performed by them in business organizations. The basic purpose of information is to inform, evaluate, persuade, and organize.

It helps in creating new concepts, identifying problems, solving problems, decision making, planning, initiating, and controlling. These are just some of the purposes to which information is directed to human activity in business organizations.

- (iii) **Mode and format:** The modes of communicating information to humans are sensory (through sight, hear, taste, touch and smell) but in business they are either visual, verbal or in written form.

Format of information should be so designed that it assists in decision making, solving problems, initiating planning, controlling and searching. Therefore, all the statistical rules of compiling statistical tables and presenting information by means of diagram, graphs, curves, etc., should be considered. Format of information dissemination is a matter of imagination and perception. It should be simple, relevant and should highlight important points but should not be too cluttered up.

- (iv) **Decay:** Value of information usually decays with time and usage and so it should be refreshed from time to time. For example, we access the running score sheet of a cricket match through Internet sites and this score sheet is continually refreshed at a fixed interval or based on status of the state. Similarly, in highly fluctuating share market a broker is always interested about the latest information of a particular stock/s.
- (v) **Rate:** The rate of transmission/reception of information may be represented by the time required to understand a particular situation. A useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive, Quantitatively, the rate for humans may be measure by the number of numeric characters transmitted per minute, such as sales reports from a district office. For machines the rate may be based on the number of bits of information per character (sign) per unit of time.
- (vi) **Frequency:** The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little changes that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.
- (vii) **Completeness:** The information should be as complete as possible. For example - Hartz's model for investment decisions provides information on mean, standard deviation and the shape of the distribution of ROI and NPV. With this complete information, the manager is in a much better position to decide whether or not to undertake the venture.

6. (a) 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 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.
- (b) **Cold Site:** If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system- raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
- Hot Site:** If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. 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 organisations that have hot-site needs.
- (c) **System Control Audit Review File (SCARF):** The system control audit review file (SCARF) technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Auditors might use SCARF to collect the following types of information:

- **Application system errors** - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and procedural variances** - Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System exception** - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical sample** -Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

- **Snapshots and extended records** - Snapshots and extended records can be written into the SCARF file and printed when required.
- **Profiling data** - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance measurement** - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

7. (a) **Data Privacy Policies:** These are given as follows:

- *Copyright Notice:* All information owned by the company and considered intellectual property, whether written, printed, or stored as data, must be labeled with a copyright notice in the following format : Copyright © 2003 [Company Name], Inc. All Rights Reserved
- *E-mail Monitoring:* All e-mail must be monitored for the following activity :
- Non-business use inflammatory, unethical, or illegal content disclosure of company confidential information large file attachments or message sizes
- *Customer Information Sharing:* Corporate customer information may not be shared with outside companies or individuals.
- *Encryption of Data Backups:* All data backups must be encrypted.
- *Encryption of Extranet Connection:* All extranet connections must use encryption to protect the privacy of the information traversing the network.
- *Data Access:* Access to corporate information, hard copy, and electronic data is restricted to individuals with a need to know for a legitimate business reason. Each individual is granted access only to those corporate information resources required for them to perform their job functions.

- (b) **Worms:** A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses.

Worms can help to sabotage systems yet they can also be used to perform some useful tasks. For example, worms can be used in the installation of a network. A worm can be inserted in a network and we can check for its presence at each node. A node, which does not indicate the presence of the worm for quite some time, can be assumed as not connected to the network.

Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive.

Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

- (c) **Emergency Plan:** The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked for example, major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an organization undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situations that evoke the plan have been identified, four aspects of the emergency plan must be articulated. First, the plan must show who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on. Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. Third, any evacuation procedures required must be specified. Fourth, return procedures (e.g., conditions that must be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

- (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) **HIPAA:** The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress in 1996. The major points of the act are given as follows:

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for 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 nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system. What is of interest here is the Security Rule issued under the Act.