

MOCK TEST PAPER – 1
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 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 modelling 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 while 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, 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.
- (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 should 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) Major weaknesses of Agile Methodology are given as follows:

- In case of some software deliverables, especially the larger ones, it is difficult to assess the efforts required at the beginning of the software development life cycle.
- There is lack of emphasis on necessary designing and documentation.

- Agile increases potential threats to business continuity and knowledge transfer. By nature, Agile projects are extremely light on documentation because the team focuses on verbal communication with the customer rather than on documents or manuals.
 - Agile requires more re-work. Because of the lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects when the various components of the software are combined and forced to interact.
 - The project can easily get taken off track if the customer representative is not clear about the final outcome that they want.
 - Only senior programmers are capable of taking the kind of decisions required during the development process. Hence, it has no place for newly appointed programmers, unless combined with experienced resources.
 - Agile lacks the attention to outside integration. Because Agile teams often do not invest the time in identifying and designing the integration points with other systems in advance, the need for an integration point can become a last-minute surprise that often requires re-work, additional time, removal from scope, or a poor-quality product.
- (b) The set of skills, which is generally expected from an IS auditor are given as follows:
- Sound knowledge of business operations, practices and compliance requirements,
 - The requisite professional technical qualification and certifications,
 - A good understanding of information Risks and Controls,
 - Knowledge of IT strategies, policy and procedure controls,
 - Ability to understand technical and manual controls relating to business continuity, and
 - Good knowledge of Professional Standards and Best practices of IT controls and security.
- (c) **[Section 22] Application for license of ITAA 2008:**
- (1) Every application for issue of a license shall be in such form as may be prescribed by the Central Government.
 - (2) Every application for issue of a license shall be accompanied by-
 - (a) a certification practice statement;
 - (b) a statement including the procedures with respect to identification of the applicant;

- (c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;
 - (d) such other documents, as may be prescribed by the Central Government.
3. (a) Major characteristic for an effective MIS are given as follows:
- **Management Oriented:** It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only, it may also meet the information requirements of middle level or operating levels of management as well.
 - **Management Directed:** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
 - **Integrated:** Development of information should be an integrated one, which means that all the functional and operational information sub-system should be tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management by taking a comprehensive view or a complete look at the inter locking sub-systems that operate within a company.
 - **Common Data Flows:** It means that the use of common input, processing and output procedures and media whenever required. Data is captured by system analysts only once and as close to its original source as possible. They, then, try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
 - **Heavy Planning Element:** An MIS usually takes 3 to 5 years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development who should keep in view future objectives and requirements of firm's information in mind.
 - **Sub System Concept:** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems which can be implemented one at a time by developing a phasing plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
 - **Common Database:** Database is the mortar that holds the functional systems together. It is defined as a "super-file" which consolidates and integrates data

records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.

- **Computerized:** Though MIS can be implemented without using a computer, the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

(b) Major compliance testing areas that should be outlined by an Audit Policy are given as follows:

- Organizational and Operational Controls,
- Security Management Controls,
- System development and Documentation Controls,
- Application Controls,
- Physical and Environmental Controls,
- Access Controls, and
- Business Continuity Controls, etc.

(c) Acquisition standards should focus on the following issues:

- Ensuring security, reliability, and functionality already built into a product.
- Ensuring managers for complete and appropriate vendor, contract, and licensing reviews and acquiring products compatible with existing systems.
- Including invitations-to-tender and request-for-proposals. Invitations-to-tender involve soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software. Request-for-proposals involve soliciting bids when acquiring off-the-shelf or third-party developed software.
- Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.

4. (a) Major points, which are emphasized by the methodology for developing a Business Continuity Plan are given as follows:

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

- Obtaining commitment from appropriate management to support and participate in the effort;
 - Defining recovery requirements from the perspective of business functions;
 - Documenting the impact of an extended loss to operations and key business functions;
 - Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
 - Selecting business continuity teams that ensure the proper balance required for plan development;
 - Developing a business continuity plan that is understandable, easy to use and maintain; and
 - Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.
- (b) Minimal issues that should be addressed by an Information Security Policy are given as follows:
- a definition of information security,
 - reasons 'why information security is important to the organization', and its goals and principles,
 - a brief explanation of the security policies, principles, standards and compliance requirements,
 - definition of all relevant information security responsibilities, and
 - reference to supporting documentation.
- (c) **Corrective Controls:** Corrective controls are to: designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A business continuity plan is considered to be a significant corrective control. The main characteristics of the corrective controls are:
- minimize the impact of the threat,
 - identify the cause of the problem,
 - remedy problems discovered by detective controls,
 - get feedback from preventive and detective controls,
 - correct error arising from a problem, and
 - modify the processing systems to minimize future occurrences of the problem.

5. (a) A practical set of principles to guide the design of measures and indicators to be included in an EIS is given as follows:
- EIS measures must be easy to understand and collect. Wherever possible, data should be collected naturally as part of the process of work. An EIS should not add substantially to the workload of managers or staff.
 - EIS measures must be based on a balanced view of the organization's objective. Data in the system should reflect the objectives of the organization in the areas of productivity, resource management, quality and customer service.
 - Performance indicators in an EIS must reflect everyone's contribution in a fair and consistent manner. Indicators should be as independent as possible from variables outside the control of managers.
 - EIS measures must encourage management and staff to share ownership of the organization's objectives. Performance indicators must promote both team-work and friendly competition. Measures will be meaningful for all staff; people must feel that they, as individuals, can contribute to improving the performance of the organization.
 - EIS information must be available to everyone in the organization. The objective is to provide everyone with useful information about the organization's performance. Information that must remain confidential should not be part of the EIS or the management system of the organization.
 - EIS measures must evolve to meet the changing needs of the organization.
- (b) The detailed controls and objectives of System Development and Maintenance with reference to Information Security Management System(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) Some of the major disadvantages and limitations of continuous audit techniques are given as under:

- Auditors should be able to obtain resources required from the organisation to support development, implementation, operation, and maintenance of continuous audit techniques.
 - Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
 - Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
 - Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
 - Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.
6. (a) Major questions, which should be answered while stating the scope under SDLC are given as follows:
- **Functionality requirements:** What functionalities will be delivered through the solution?
 - **Data to be processed:** What data is required to achieve these functionalities?
 - **Control requirements:** What are the control requirements for this application?
 - **Performance requirements:** What level of response time, execution time and throughput is required?
 - **Constraints:** What are the conditions the input data has to conform to? For example, what is the maximum number of characters that a name can have in a database?
 - **Interfaces:** Is there any special hardware/software that the application has to interface with? For example Payroll application may have to capture from the attendance monitoring system that the company has already installed. Then, the solution developer has to understand the format of data, frequency mode of data transfer and other aspects of the software.
 - **Reliability requirements:** Reliability of an application is measured by its ability to remain uncorrupted in the face of inadvertent / deliberate misuse. The reliability required for an application depends on its criticality and the user profile.
- (b) Major categories of the risk management strategies 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. For example, 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. For example, 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.

- (c) **Level 5 - Optimizing Level of CMM:** At the Optimizing Level, the entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. Innovations that exploit the best software engineering practices are identified and transferred throughout the organization.

Software project teams in Level 5 organizations analyze defects to determine their causes. Software processes are evaluated to prevent known types of defects from recurring, and lessons learned are disseminated to other projects. There is chronic waste, in the form of rework, in any system simply due to random variation. Waste is unacceptable; organized efforts to remove waste result in changing the system, i.e., improving the process by changing "common causes" of inefficiency to prevent the waste from occurring. While this is true of all the maturity levels, it is the focus of Level 5.

The software process capability of Level 5 organizations can be characterized as continuously improving because Level 5 organizations are continuously striving to improve the range of their process capability, thereby improving the process performance of their projects. Improvement occurs both by incremental advancements in the existing process and by innovations using new technologies

and methods. Technology and process improvements are planned and managed as ordinary business activities.

7. (a) **Proxy Server Firewalls:** Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network. Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices. The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate proxy server. Common proxy servers are the domain name server (DNS), Web server (HTTP), and mail (SMTP) server. Proxy servers frequently cache requests and responses, providing potential performance benefits.

Additionally, proxy servers provide another layer of access control by segregating the flow of Internet traffic to support additional authentication and logging capability, as well as content filtering. Web and e-mail proxy servers, for example, are capable of filtering for potential malicious code and application-specific commands. They may implement anti-virus and anti-spam filtering, disallow connections to potentially malicious servers, and disallow the downloading of files in accordance with the institution's security policy.

Proxy servers are increasing in importance as protocols are tunneled through other protocols. For example, a protocol-aware proxy may be designed to allow Web server requests to port 80 of an external Web server, but disallow other protocols encapsulated in the port 80 requests.

- (b) **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.
- (c) **Scoring Approach for Risk Assessment:** In the Scoring approach the risks in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.
- (d) **'Acquire and Implement' domain of COBIT:** 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

- (e) **Data Dictionary:** A data dictionary is a computer file that contains descriptive information about the data items in the files of a business information system. Thus, a data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in a business information system. This information may include:
- Codes describing the data item's length (in characters), data type (alphabetic, numeric, alphanumeric, etc.), and range (e.g., values from 1 to 99 for a department code).
 - The identity of the source document(s) used to create the data item.
 - The names of the computer files that store the data item.
 - The names of the computer programs that modify the data item.
 - The identity of the computer programs or individuals permitted to access the data item for the purpose of file maintenance, upkeep, or inquiry.
 - The identity of the computer programs or individuals not permitted to access the data item.