

MOCK TEST PAPER – 1
FINAL COURSE: GROUP – II
PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT
SUGGESTED ANSWERS/HINTS

1. (a) To qualify for a true ERP solution, a system has to possess the following characteristics :
- ◆ **Flexibility:** An ERP system should be flexible to respond to the changing needs of an enterprise. The client server technology enables ERP to run across various database back ends through Open Database Connectivity (ODBC).
 - ◆ **Modular & Open:** ERP system has to have open system architecture. This means that any module can be interfaced or detached whenever required without affecting the other modules. It should support multiple hardware platforms for the companies having heterogeneous collection of systems. It must support some third party add-ons also.
 - ◆ **Comprehensive:** It should be able to support variety of organizational functions and must be suitable for a wide range of business organizations.
 - ◆ **Beyond The Company:** It should not be confined to the organizational boundaries, rather it should support the on-line connectivity to the other business entities of the organization.
 - ◆ **Best Business Practices:** It must have a collection of the best business processes applicable worldwide. An ERP package imposes its own logic on a company's strategy, culture and organization.
- (b) The detailed controls and objectives of access control are given as follows:
- ◆ *Business requirement for access control:* To control access to information;
 - ◆ *User access management:* To prevent unauthorized access to information systems;
 - ◆ *User responsibilities:* To prevent unauthorized user access;
 - ◆ *Network access control:* To protect 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 teleworking:* To ensure information security when using

mobile computing & teleworking facilities.

(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.

(d) Major tasks that are to be performed during the post-implementation phase of an ERP package are given as follows:

- ◆ To develop the new job descriptions and organization structure to suit the post ERP scenario;
- ◆ To determine the skill gap between existing jobs and envisioned jobs;
- ◆ To assess training requirements, and create and implement a training plan;
- ◆ To develop and amend HR, financial and operational policies to suit the future ERP environment; and
- ◆ To develop a plan for workforce logistics adjustment.

2. **(a)** Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. Enough information should be assembled so that a qualified person can understand the present system without visiting any of the operating departments. Review of existing methods, procedures, data flow, outputs, files, inputs and internal controls should be intensive in order to fully understand the present system and its related problems.

The following areas may be studied in depth:

- ◆ **Review historical aspects:** A brief history of the organization is a logical starting point for the analysis of the present system. The historical facts should

identify the major turning points and milestones that have influenced its growth. A review of annual reports can provide an excellent historical perspective. A historical review of the organization chart can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should identify what system changes have occurred in the past. These should include operations that have been successful or unsuccessful with computer equipment and techniques.

- ◆ **Analyze inputs:** A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of the various sources from where the data can be initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations. If the analyst investigates these questions thoroughly, s/he will be able to determine how these inputs fit into the framework of the present system.
- ◆ **Review data files maintained:** The analysts should investigate the data files maintained by each department by noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. Information on common data files and their size will be an important factor, which will influence the new information system. This information may be contained in the systems and procedures manuals. The system analyst should also review all online and offline files, which are maintained in the organization as these will reveal information about data that are not contained in any output. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.
- ◆ **Review methods, procedures and data communications:** Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure's review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement in opportunities in the present information system. A system analyst also needs to review and understand the present data communications used by the organization. S/he must review the types of data communication equipment including data interface, data links, modems, dial-up and leased lines and multiplexers. The system analyst must understand how the data communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.

- ◆ **Analyze outputs:** The outputs or reports should be scrutinized carefully by the system analysts in order to determine 'how well they will meet the organization's needs'. The analysts must understand 'what information is needed' and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting it is used, how long it is kept on file, etc. must be investigated. Often many reports are a carryover from earlier days and have little relevance to current operations. Attempt should be made to eliminate all such reports in the new system.
- ◆ **Review internal controls:** A detailed investigation of the present information system is not complete until internal controls are reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal control may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipment might allow much greater control over the data.
- ◆ **Model the existing physical system and logical system:** As the logic of inputs, methods, procedures, data files, data communications, reports, internal control and other important items are reviewed and analyzed in a top down manner, the process must be properly documented. The logical flow of the present information system may be depicted with the help of system flow charts. The physical flow of the existing system may be shown by employing data flow diagrams. During the process of developing the data flow diagram, work on data dictionary for the new information system should be begun. The data elements needed in the new system will be found in the present system only. Hence, it is wise to start the development of the data dictionary as early as possible.
- ◆ The flow charting and diagramming of present information not only organizes the facts, but also helps disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.
- ◆ **Undertake overall analysis of present system:** Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of:
 - the present work volume,
 - the current personnel requirements, and
 - the present benefits and costs.

Each of these must be investigated thoroughly.

(b) 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.

(c) "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Chapter-II, Section 3 of Information Technology (Amendment) Act 2008 provides conditions subject to which an electronic record is authenticated by means of affixing digital signature. The section is given as follows:

[Section 3] Authentication of Electronic Records:

- (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.
- (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the

initial electronic record into another electronic record.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
 - (b) that two electronic records can produce the same hash result using the algorithm.
- (3) Any person by the use of a public key of the subscriber can verify the electronic record.
 - (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

3. (a) The major limitations of MIS are given as follows :

- The quality of the outputs of MIS is basically governed by the quantity of input and processes.
- MIS is not a substitute for effective management, which means that it cannot replace managerial judgment in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for the purpose of every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives.
- MIS is less useful for making non-programmed decisions. Such type of decisions is not of the routine type and thus requires information, which may not be available from existing MIS to executives.
- The effectiveness of MIS is reduced in organizations, where the culture of hoarding information and not sharing with other holds.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

- (b) An Information Security Policy should address the following major issues:
- ◆ 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) Major strengths of agile methodologies are given as follows:
- ◆ Agile methodology has the concept of an adaptive team, which is able to respond to the changing requirements.
 - ◆ The team does not have to invest time and effort and finally find that by the time they deliver the product, the requirement of the customer has changed.
 - ◆ Face to face communication and continuous inputs from customer representative leaves no space for guesswork.
 - ◆ The documentation is crisp and to the point to save time.
 - ◆ The end result is the high quality software in least possible time duration and satisfied customer.

4. (a) **Business Impact Analysis** : Business Impact Analysis (BIA) is a process of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.

The business impact analysis is intended to help and understand the degree of potential loss (and various other unwanted effects) which could occur. This will cover not only direct financial loss, but other issues also, such as reputation damage, regulatory effects, etc.

Major tasks are to be undertaken in this phase as enumerated under:

- (i) 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.
- (ii) Identify critical business processes.
- (iii) Identify and quantify threats/ risks to critical business processes both in terms

of outage and financial impact.

- (iv) Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
- (v) Determine the maximum allowable downtime for each business process.
- (vi) Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
- (vii) Determine the impact to the organisation in the event of a disaster, e.g. financial reputation, etc.

(b) Components of the Security Policy: A good security policy should clearly state the following:

- ◆ Purpose and scope of the document and the intended audience;
- ◆ The security infrastructure.
- ◆ Security policy document maintenance and compliance requirements;
- ◆ Incident response mechanism and incident reporting;
- ◆ Security organization structure;
- ◆ Inventory and classification of assets;
- ◆ Description of technologies and computing structure;
- ◆ Physical and environmental security;
- ◆ Identify management and access control;
- ◆ IT operations management;
- ◆ IT communications;
- ◆ System development and maintenance controls;
- ◆ Business continuity planning;
- ◆ Legal compliances;
- ◆ Monitoring and Auditing Requirements; and.
- ◆ Underlying technical policy.

(c) The set of major skills that is generally expected from an IS auditor include:

- ◆ Sound knowledge of business operations, practices and compliance requirements,
- ◆ Should possess the requisite professional technical qualification and certifications,
- ◆ An 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.

5. (a) **Executive Information Systems (EIS):** An **Executive Information System (EIS)** – sometimes referred to as an Executive Support System (ESS) – is a DSS that is designed to meet the special needs of top-level managers. Some people use the terms “EIS” and “ESS” interchangeably, but others do not. Any distinction between the two usually is because Executive Support Systems are likely to incorporate additional capabilities such as electronic mail.

Major characteristics of EIS are given as follows :

- ◆ EIS is a Computer-based-information system that serves the information need of top executives.
 - ◆ EIS enables users to extract summary data and model complex problems without the need to learn query languages statistical formulas or high computing skills.
 - ◆ EIS provides rapid access to timely information and direct access to management reports.
 - ◆ EIS is capable of accessing both internal and external data.
 - ◆ EIS provides extensive online analysis tool like trend analysis, market conditions etc.
 - ◆ EIS can easily be given a DSS support for decision making.
- (b) An IS auditor should keep the following points in mind while working with logical access control mechanisms.
- (i) Reviewing the relevant documents pertaining to logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system.
 - (ii) The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency.
 - (iii) Deficiencies or redundancies must be identified and evaluated.
 - (iv) By supplying appropriate audit techniques, s/he must be in a position to verify test controls over access paths to determine its effective functioning.
 - (v) S/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.

- (vi) The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.
- (c) Some of the 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/s 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.
- 6. (a) Various fact-finding techniques, which are used by the system analysts for determining the requirements of a system, are given as follows :
 - ◆ **Documents:** Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc. Documents are a very good source of information about user needs and the current system.
 - ◆ **Questionnaires:** Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.
 - ◆ **Interviews:** Users and managers may also be interviewed to extract information in-depth. The data gathered through interviews often provide system developers with a complete picture of the problems and opportunities. Interviews also give analysts the opportunity to note user reaction first-hand and to probe for further information.
 - ◆ **Observation:** In prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototypes of a

new system, the system can be successfully developed.

- (b) **Systematic risks:** These risks are unavoidable risks; these are constant across majority of technologies and applications. For example, the probability of power outage is not dependant on the industry but is dependent on external factors. Systematic risks would remain, no matter what technology is used. Thus efforts to seek technological solution to reduce systematic risks would essentially be unfruitful activity and needs to be avoided. Systematic risks can be reduced by designing management control process and does not involve technological solutions. For example, the solution to non availability of consumable is maintaining a high stock of the same. Thus, a systematic risk can be mitigated not by technology but by management process. Hence, one would not make any additional payment for technological solution to the problem. To put in other words, there would not be any technology linked premium that one should pay trying to reduce the exposure to systematic risk.

Unsystematic risks: These risks are those, which are peculiar to the specific applications or technology. One of the major characteristics of these risks would be that they can be generally mitigated by using an advanced technology or system. For example, one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. Thus, by making additional investment, one can mitigate these unsystematic risks.

- (c) **Level 1 - The Initial Level of CMM:** At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. Such organizations frequently have difficulty for making commitments that the staff can meet with an orderly engineering process, resulting in a series of crises. During a crisis, projects typically abandon planned procedures and revert to coding and testing. Success depends entirely on having an exceptional manager and a seasoned and effective software team. Occasionally, capable and forceful software managers can withstand the pressures to take shortcuts in the software process; but when they leave the project, their stabilizing influence leaves with them. Even a strong engineering process cannot overcome the instability created by the absence of sound management practices. In spite of this ad hoc, even chaotic, process, Level 1 organizations frequently develop products that work, even though they may be over the budget and schedule. Success in Level 1 organizations depends on the competence and heroics of the people in the organization and cannot be repeated unless the same competent individuals are assigned to the next project. Thus, at Level 1, capability is a characteristic of the individuals, not of the organization.
7. (a) **Corrective Controls:** Corrective controls are 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 (BCP) 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.

Examples of Corrective Controls are: Contingency planning, Backup procedure, Rerun procedures, Treatment procedures for a disease, Change input value to an application system, and investigate budget variance and report violations.

- (b) **White Box Testing: White box testing** uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. Since the tests are based on the actual implementation, if the implementation changes, the tests probably will need to change, too. It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit. While, it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.
- (c) **Delphi Technique for Risk Assessment:** This technique was first used by the Rand Corporation for obtaining a consensus opinion. Here, a panel of experts is appointed. Each expert gives his/her 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 by taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.
- (d) **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. Security Rule issued under the Act is the key component of the Act.

- (e) **Phased implementation:** With this strategy, implementation can be staged with conversion to the new system taking place by degrees. For example - some new files may be converted and used by employees whilst other files continue to be used on the old system i.e. the new is brought in stages (phases). If each phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one as shown in the following Fig.

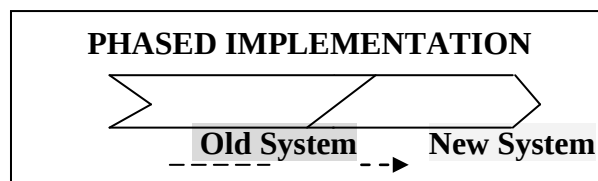


Fig. : Phased Implementation