Test Series: February, 2016

MOCK TEST PAPER – 1

FINAL COURSE: GROUP – II

PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT

SUGGESTED ANSWERS/HINTS

1. (a) Two primary methods through which the analyst would have collected the data are given as follows:

- Reviewing Internal Documents: The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project. For example, to review an inventory system proposal, an analyst may try to know how does the inventory department operates and who are the managers and supervisors. Analysts can usually learn these details by examining organization charts and studying written operating procedures.
- Conducting Interviews: Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it. Usually, preliminary investigation interviews involve only management and supervisory personnel.

(b) Section 7, Chapter III of Information Technology Act, 2000 is "*Retention of Electronic Records"* which states that -

(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, if -

(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:

PROVIDED that 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.

(b) The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- Financial Loss: Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.
- Legal Repercussions: Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
- Loss of credibility or Competitive Edge: News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility. There have been instances where share prices of such companies went down, as the news of such attach percolated to the market.
- Disclosure of Confidential, Sensitive or Embarrassing Information: Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.
- Sabotage: The above situation may lead to misuse of such information by enemy country.

2. (a) Integration Testing: Integration testing is an activity of software testing in which individual software modules are combined and tested as a group. It occurs after unit testing and before system testing with an objective to evaluate the validity of connection of two or more components that pass information from one area to another. Integration testing takes as its input modules that have been unit tested, groups them in larger aggregates, applies tests defined in an integration test plan to those aggregates, and delivers as its output the integrated system ready for system testing. This is carried out in the following two manners:

- Bottom-up Integration: It is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub-system testing, and then testing of the entire system.

Bottom-up testing is easy to implement as at the time of module testing, tested subordinate modules are available. The disadvantage however is that testing of major decision / control points is deferred to a later period.

- Top-down Integration: It starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module. An incomplete portion of a program code that is put under a function in order to allow the function and the program to be compiled and tested is referred to as a stub. A stub does not go into the details of implementing details of the function or the program being executed.

  Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested with stubs. This process continues till the atomic modules are reached. Since decision-making processes are likely to occur in the higher levels of program hierarchy, the top-down strategy emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes. The difficulty arises in the top-down method, because the high-level modules are tested, not with real outputs from subordinate modules, but from stubs.

(b) Physical Access Controls: These are the controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc.

These controls are personnel; hardware and software related and include procedures exercised on access to IT resources by employees/outsiders. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy.

These Physical security and access controls should address supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to authorized individuals where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism. Further, IT management should ensure zero visibility.

Logical Access Controls: These are the controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc. Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and incident

handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting.

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

(c) Audit trails can be used to support security objectives in three ways:

- Detecting Unauthorized Access: Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm.
- Reconstructing Events: Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Audit trail analysis also plays an important role in accounting control.
- Personal Accountability: Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

3. (a) The primary objective of a business continuity plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- Provide the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort; and
- Identify critical lines of business and supporting functions.

The goals of the business continuity plan should be to:

- Identify weaknesses and implement a disaster prevention program;
- minimize the duration of a serious disruption to business operations;
- facilitate effective co-ordination of recovery tasks; and
- reduce the complexity of the recovery effort.

(b) The main categories of Social Networks are as below:

- Social Contact Networks: These types of networks are formed to keep contact with friends and family. These have become the most popular sites on the network today. They have all components of Web 2.0 like blogging, tagging, wikis, and forums. Examples of these include Orkut, Facebook and Twitter.
- Study Circles: These are social networks dedicated for students, where they can have areas dedicated to student study topics, placement related queries and advanced research opportunity gathering. These have components like blogging and file sharing. Examples of these include Fledge Wing and College Tonight.
- Social Networks for Specialist Groups: These types of social networks are specifically designed for core field workers like doctors, scientists, engineers, members of the corporate industries. A very good example for this type of network is LinkedIn.
- Networks for Fine Arts: These types of social networks are dedicated to people linked with music, painting and related arts and have lots of useful networking information for all aspiring people of the same line.
- Police and Military Networks: These types of networks, though not on a public domain, operate much like social networks on a private domain due to the confidentiality of information.
- Sporting Networks: These types of social networks are dedicated to people of the sporting fraternity and have a gamut of information related to this field. Examples of these include Athlinks.
- Mixed Networks: There are a number of social networks that have a subscription of people from all the above groups and is a heterogeneous social network serving multiple types of social collaboration.
- Social Networks for the 'inventors': These are the social networks for the people who have invented the concept of social networks, the very developers and architects that have developed the social networks. Examples include Technical Forums and Mashup centres.

- Shopping and Utility Service Networks: The present world of huge consumerism has triggered people to invest in social networks, which will try to analyze the social behaviour and send related information for the same to respective marts and stores.
- Others: Apart from the networks outlined above, there are multiple other social networks, which serve huge number of the internet population in multiple ways. Some of these networks die out very fast due to lack of constructive sustenance thoughts while others finally migrate to a more specialist network.

(c) Feasibility Study: In SDLC; after possible solution options are identified, project feasibility i.e. the likelihood that these systems will be useful for the organization is determined. A feasibility study is carried out by the system analysts, which refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. The Feasibility Study of a system is evaluated under following dimensions described briefly as follows:

- Technical: Is the technology needed available?
- Financial: Is the solution viable financially?
- Economic: Return on Investment?
- Schedule/Time: Can the system be delivered on time?
- Resources: Are human resources reluctant for the solution?
- Operational: How will the solution work?
- Behavioral: Is the solution going to bring any adverse effect on quality of work life?
- Legal: Is the solution valid in legal terms?

4. (a) Impact of Technology on Internal Controls is as below:

- Competent and Trustworthy Personnel: Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the errors responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations.
- Segregation of Duties: In a manual system, during the processing of a transaction, there are split between different people, such that one person does not process a transaction right from start to finish. Various stages in the transaction cycle are spread between two or more individuals. However, in a computerised system, the auditor should also be concerned with the segregation of duties within the IT department. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of

the interrelationship between the source of data, how it is processed and distribution and use of output.

- Authorization Procedures: In manual systems, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
- Adequate Documents and Records: In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system. In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available to trance the transactions in a computerized system. However, if the controls over the protection and storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.
- Physical Control over Assets and Records: In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster.
- Adequate Management Supervision: In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location. In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried our remotely. The Management's supervision and review helps to deter and detect both errors and fraud.
- Independent Checks on Performance: In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures. If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.

- Comparing Recorded Accountability with Assets: Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. a computer system, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies o the data being prepared for comparison purposes.
- Delegation of Authority and Responsibility: A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

(b) The key governance practices of Governance of Enterprise IT (GEIT) area as follows:

- Evaluate the Governance System: Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;
- Direct the Governance System: Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making; and
- Monitor the Governance System: Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

(c) Detective Controls: These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend. The main characteristics of such controls are given as follows:

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc;
- An established mechanism to refer the reported unlawful activities to the appropriate person or group;

- Interaction with the preventive control to prevent such acts from occurring; and
- Surprise checks by supervisor.

Examples of detective controls include Hash totals, Check points in production jobs, Echo control in telecommunications, Error message over tape labels, Duplicate checking of calculations, Periodic performance reporting with variances, Past-due accounts report, The internal audit functions, Intrusion detection system, Cash counts and bank reconciliation, and Monitoring expenditures against budgeted amount.

5. (a) Expert System - An Expert System is highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – how much can be invested. Does the client have any preferences regarding specific types of securities? And so on.

A characteristic of Expert Systems is the ability to declare or explain the reasoning process that was used to make decisions. Some of the business applications of Expert System are as follows:

- Accounting and Finance - It provides tax advice and assistance, helping with credit- authorization decisions, selecting forecasting models, providing investment advice.
- Marketing - It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.
- Manufacturing - It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.
- Personnel - It is useful in assessing applicant qualifications, giving employees assisting at filling out forms.
- General Business - It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

(b) Operating system performs the following major tasks:

- Scheduling Jobs: They can determine the sequence in which jobs are executed, using priorities established.

- Managing Hardware and Software Resources: They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.
- Maintaining System Security: They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.
- Enabling Multiple User Resource Sharing: They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.
- Handling Interrupts: An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed. Interrupts are issued when a program requests an operation that does not require the CPU, such as input or output, or when the program exceeds some predetermined time limit.
- Maintaining Usage Records: They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output devices. Such information is usually maintained for the purpose of charging users' departments for their use of the organization's computing resources.

(c) Major advantages of continuous audit techniques are given as follows:

- Timely, Comprehensive and Detailed Auditing – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed 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.

6. (a) Various types of back-ups used in Business Continuity Planning (BCP) are as follows:

- Full Backup: A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.
- 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 probably includes files that were already included in earlier differential backups.
- Mirror back-up: A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

(b) Information Systems Audit has been categorized into five types:

(i) Systems and Application: An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) Information Processing Facilities: An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

(iii) Systems Development: An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for

systems development.

(iv) Management of IT and Enterprise Architecture: An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

(v) Telecommunications, Intranets, and Extranets: An audit to verify that controls are in place on the client (end point device), server, and on the network connecting the clients and servers.

(c) Corporate Governance or Conformance: Corporate Governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The corporate governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.

Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital.

Corporate Governance drives the corporate information needs to meet business objectives. Good corporate governance requires sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of Audit Committee, risk management and compliance with the relevant laws and standards including corporate disclosure requirements. Corporate governance is necessary for the purpose of monitoring and measuring their performance.

7. (a) Following are the major misconceptions about Management Information Systems (MIS):

- Any computer based information system is a MIS;
- Any reporting system is MIS;
- MIS is a management technique;
- MIS is a bunch of technologies;
- MIS is an implementation of organizational systems and procedures. It is a file structure;
- The study of MIS is about use of computers; and
- More data in generated reports refers more information to managers.

- Accuracy plays vital role in reporting.

(b) Major Data Integrity policies are given as under:

- Virus-Signature Updating: Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- Software Testing: All software must be tested in a suitable test environment before installation on production systems.
- Division of Environments: The division of environments into Development, Test, and Production is required for critical systems.
- Offsite Backup Storage: Backups older than one month must be sent offsite for permanent storage.
- Quarter-End and Year-End Backups: Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes
- Disaster Recovery: A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

(c) The PDCA Cyclic Process under ISO 27001 is as follows:

- The Plan Phase – This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
- The Do Phase – This phase includes carrying out everything that was planned during the previous phase.
- The Check Phase – The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.
- The Act Phase – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

(d) Communication as a Service (CaaS) in Cloud Computing: CaaS is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates the large capital investments. Examples are: Voice over IP (VoIP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.

(e) Weaknesses of the Spiral Model: Some of the weaknesses identified by the experts and practitioners include the following:

- It is challenging to determine the exact composition of development methodologies to use for each iteration around the Spiral.
- It may prove highly customized to each project, and thus is quite complex and limits reusability.
- A skilled and experienced project manager is required to determine how to apply it to any given project.
- No established controls exist for moving from one cycle to another cycle. Without controls, each cycle may generate more work for the next cycle.
- There are no firm deadlines, cycles continue with no clear termination condition leading to, inherent risk of not meeting budget or schedule.