MOCK TEST PAPER 1

FINAL COURSE (OLD) GROUP - II

PAPER - 6: INFORMATION SYSTEMS CONTROL AND AUDIT

ANSWERS

Division A: MULTIPLE CHOICE QUESTIONS

1. **(c)** Vulnerability
2. **(d)** Reliability
3. **(a)** Preventative Control
4. **(b)** Test Plan
5. **(c)** Business Analyst
6. **(a)** Confidentiality
7. **(b)** Mr. X and Directors
8. **(c)** Infrastructure as a Service (IaaS)
9. **(d)** The Project Manager should work independently from the Steering Committee in finalizing the detailed work plan and developing interview schedules.
10. **(a)** owners/shareholders, Board of Directors, its chairman, managing director, or the chief executive
11. **(a)** (i), (ii), (iii)
12. **(d)** Incremental Backup consumes the most storage space as compared to full and differential backups
13. **(b)** Cost Analysis
14. **(c)** Processing Controls
15. **(d)** Subscriber
16. **(c)** Bandwidth
17. **(b)** Counter Measure
18. **(d)** Decision Making
19. **(c)** Security Administration
20. **(d)** Performance Analysis Report
21. **(d)** Incremental
22. **(a)** Flowchart

Division B: DESCRIPTIVE QUESTIONS

1. **(a)** **COBIT 5** is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies; and helps these enterprises to create optimal value from their information and technology.

   Components in COBIT 5 are as follows:

   - **Framework -** Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;

- **Process Descriptions -** A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- **Control Objectives -** Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
- **Management Guidelines -** Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.
- **Maturity Models -** Assess maturity and capability per process and helps to address gaps.

(b) Some of the major ways of protecting the installation against fire damage in an organization are as follows:

- Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this.
- Besides the control panel, master switches may be installed for power and automatic fire suppression system. Different fire suppression techniques like Dry-pipe sprinkling systems, water based systems, halon etc., depending upon the situation may be used.
- Manual fire extinguishers can be placed at strategic locations.
- Fireproof Walls, Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials such as wastebaskets, curtains, desks and cabinets should be used.
- Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
- All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented are Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers.
- Less Wood and plastic should be in computer rooms.
- Use a gas based fire suppression system;
- To reduce the risk of firing, the location of the computer room should be strategically planned and should not be located in the basement or ground floor of a multi-storey building.
- Regular Inspection by Fire Department should be conducted.
- Fire repression systems should be supplemented and not replaced by smoke detectors.
- **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation. In all circumstances saving human life should be given paramount importance.
- **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station).
- **Wiring Placed in Electrical Panels and Conduit:** Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised floor in the computer room.

(c) The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor. The set of skills that is generally expected to be with an IS auditor include:

- Sound knowledge of business operations, practices and compliance requirements;
- Should possess the requisite professional technical qualification and certifications;
- A good understanding of information Risks and Controls;
- Knowledge of IT strategies, policy and procedural 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.

2. (a) Application security audit uses the Layered approach which is based on the activities being undertaken at various levels of management namely Operational, Tactical and Strategic Various aspects relating to these layers are as follows:

(i) **Operational Layer:** The operational layer audit issues include:

- **User Accounts and Access Rights:** This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities. Auditor needs to always ensure the use of unique user IDs, and this needs to be traceable to individual for whom it is created.
- **Password Controls:** In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum. Auditor needs to check whether there are applications where password controls are weak.
- **Segregation of Duties:** Segregation of Duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals' responsibility for initiating and recording transactions and custody of assets to separate individuals. Auditor needs to check that there is no violation of this. Any violation may have serious repercussions, the same need to be immediately communicated to those charged with governance.

(ii) **Tactical Layer:** At the tactical layer, security administration is put in place. This includes:

- Timely updates to user profiles, like creating/deleting and changing of user accounts. Auditor needs to check that any change to user rights is a formal process including approval from manager of the employee.
- **IT Risk Management:** This function is another important function performed, it includes the following activities:
  - Assessing risk over key application controls;
  - Conducting a regular security awareness programme on application user;
  - Enabling application users to perform a self-assessment/complete compliance checklist questionnaire to gauge the users' understanding about application security;
  - Reviewing application patches before deployment and regularly monitoring critical application logs;
  - Monitoring peripheral security in terms of updating antivirus software;

An auditor should understand the risk associated with each application and obtain a report on periodic risk assessment on the application or self-assessment/ compliance reports on the application.

- **Interface Security:** This relates to application interfaced with another application in an organization. An auditor needs to understand that data flow to and from the application.

- **Audit Logging and Monitoring:** Regular monitoring the audit logs is required. The same is not possible for all transactions, so must be done on an exception reporting basis.

(iii) **Strategic Layer:** At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting. A comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security. The security policy should be supported and supplemented by detailed standards and guidelines. These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.

(b) Various processes that are mapped in Business Continuity Management (BCM) are as follows:

- **Organization Structure:** The organization should nominate a person or a team with appropriate seniority and authority to be accountable for BCM policy implementation and maintenance. It should clearly define the persons responsible for business continuity within the enterprise and responsibility.
- **Implementing Business Continuity in the Enterprise and Maintenance:** In establishing and implementing the BCM system in the organization, managers from each function on site represent their areas of the operation. These people are also responsible for the ongoing operation and maintenance of the system within their area of responsibility. Where training is required to enable as a colleague to effectively carry out their BCM responsibilities, this will be identified as part of the ongoing staff appraisal and training process. Top management should appoint the Manager (BCM) role as being the role that is responsible for the BCM policy and its implementation.

  In implementation, the major activities that should be carried out include:

  - Defining the scope and context;
  - Defining roles and responsibilities;
  - Engaging and involving all stakeholders;
  - Testing of program on regular basis;
  - Maintaining the currency & appropriateness of business continuity program;
  - Reviewing, reworking and updating the business continuity capability, risk assessments (RA) and Business Impact Analysis (BIAs);
  - Managing costs and benefits associated; and Convert policies and strategies into action.
- **BCM Documentation and Records:** All documents that form the BCM are subject to the document control and record control processes. The following documents (representative only) are classified as being part of the business continuity management system:
  - The business continuity policy;
  - The business continuity management system;
  - The business impact analysis report;
  - The risk assessment report;
  - The aims and objectives of each function;
  - The activities undertaken by each function;
  - The business continuity strategies;
  - The overall and specific incident management plans;

- The business continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training program.

(c) An IS auditor is responsible to evaluate the following while reviewing the adequacy of data security controls:

- Who is responsible for the accuracy of the data?
- Who is permitted to update data?
- Who is permitted to read and use the data?
- Who is responsible for determining who can read and update the data?
- Who controls the security of the data?
- If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
- Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?

3. (a) Some important attributes of useful and effective information are given as follows:

- **Availability -** It is a very important aspect of information. Information is useless if it is not available at the time of need. Database is a collection of files which is collection of records and data from where the required information is derived for useful purpose.
- **Purpose/Objective -** Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data. Depending upon the activities in an organization the Information communicated to people has a purpose. The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.
- **Mode and format -** The modes of communicating information to humans should be in such a way that it can be easily understandable by the people. The mode may be in the form of voice, text and combination of these two. Format also plays an important role in communicating the idea. It should be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information the different formats can be used e.g. diagrams, graphs, curves are best suited for representing the statistical data. Format of information should be simple, relevant and should highlight important points but should not be too cluttered up.
- **Current/Updated -** The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed interval of time so that the current score will be available. Similar is the case with broker who wants the latest information about the stock market.
- **Rate -** The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Useful information is the one which is

transmitted at a rate which matches with the rate at which the recipient wants to receive. For example- the information available from internet site should be available at a click of mouse.

- **Frequency -** The frequency with which information is transmitted or received affects its value. For example- the weekly reports of sales show little change as compared to the quarterly and contribute less for accessing salesman capability.
- **Completeness and Adequacy -** The information provided should be complete and adequate in itself because only complete information can be used in policy making. For example-the position of student in a class can be find out only after having the information of the marks of all students and the total number of students in a class.
- **Reliability -** It is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
- **Validity -** It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee supports in evaluating his performance.
- **Quality -** It means the correctness of information. For example, an over-optimistic manager may give too high estimates of the profit of product which may create problem in inventory and marketing.
- **Transparency -** It is essential in decision and policy making. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.
- **Value of Information -** It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

(b) Audit Trail: Audit trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning.

In Processing Controls, the audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.

Accounting Audit Trail

- To trace and replicate the processing performed on a data item.
- Triggered transactions to monitor input data entry, intermediate results and output data values.

Operations Audit Trail

- A comprehensive log on hardware consumption – CPU time used, secondary storage space used, and communication facilities used.
- A comprehensive log on software consumption – compilers used, subroutine libraries used, file management facilities used, and communication software used.

(c) For an organization to adopt ISO 27001 standard, it requires that management:

- systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

4. (a) **Hybrid Cloud** is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used. The hybrid cloud can be regarded as a private cloud extended to the public cloud and aims at utilizing the power of the public cloud by retaining the properties of the private cloud. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

Characteristics of Hybrid Cloud are as follows:

- **Scalable:** The hybrid cloud has the property of public cloud with a private cloud environment and as the public cloud is scalable; the hybrid cloud with the help of its public counterpart is also scalable.
- **Partially Secure:** The private cloud is considered as secured and public cloud has high risk of security breach. The hybrid cloud thus cannot be fully termed as secure but as partially secure.
- **Stringent Service Level Agreements (SLAs):** Overall the SLAs are more stringent than the private cloud and might be as per the public cloud service providers.
- **Complex Cloud Management:** Cloud management is complex as it involves more than one type of deployment models and also the number of users is high.

The Advantages of Hybrid Cloud include the following:

- It is highly scalable and gives the power of both private and public clouds.
- It provides better security than the public cloud.

(b) In systems that use physical source documents to initiate transactions, careful Source Document controls must be exercised over these instruments. Source document fraud can be used to remove assets from the organization. To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below:

- **Use pre-numbered source documents:** Source documents should come pre-numbered from the printer with a unique sequential number on each document. Source document numbers enable accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.
- **Use source documents in sequence:** Source documents should be distributed to the users and used in sequence. This requires the adequate physical security be maintained over the source document inventory at the user site. When not in use, documents should be kept under lock and key and access to source documents should be limited to authorized persons.

- **Periodically audit source documents:** Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.

(c) **BCP Manual:** A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. An incident or disaster affecting critical business operations can strike at any time. Successful organizations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity

The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liasioning teams between the functional area(s) affected and other departments providing support services.

5. **(a)** As per given facts, Proposal and acceptance of the proposal giving rise to an agreement was there between the ABC Ltd. and X manufacturer for the supply of dress material @ Rs. 500 per meter within 2 months from the date of order through the communication vide mails. However, in the meantime, ABC Ltd. accepted the proposal of M/s PRQ and revoked the agreement made with X manufacturer and communicated the revocation of the acceptance of the proposal.

The given situation can be dealt with the Section 10A of the IT Act, 2000, where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

Thus, accordingly following are the answers to the questions:

(i) Acceptance of offer by ABC Ltd. with X manufacturer, to the supply of dress material for the staff uniform is legal binding agreement, thus giving rise to valid contract though made through communications vide mails.

(ii) No, because provision explicitly states that contract formation in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose. So, the contention of the ABC Ltd. that no formal agreement was entered between them, is not justified.

(iii) The contract made between ABC Ltd. and the M/s PRQ cannot come into legal enforcement until the first contract i.e. contract between ABC Ltd. and X manufacturer discharged or performed. Here in the case neither was the case. Further, the contract cannot be revoked once it is accepted. In fact, it is the breach of the contract. Due to the breach of the contract the ABC Ltd.is liable for damages to the X manufacturer.

(b) Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit. Continuous auditing has a number of potential benefits including:

- Reducing the cost of the basic audit assignment by enabling auditors to test a larger sample (up to 100 percent) of client's transactions and examine data faster and more efficiently than the manual testing required when auditing around the computer;
- Reducing the amount of time and costs auditors traditionally spend on manual examination of transactions;

- Increasing the quality of audits by allowing auditors to focus more on understanding a client's business and industry and its internal control structure; and
- Specifying transaction selection criteria to choose transactions and perform both tests of controls and substantive tests throughout the year on an ongoing basis.

(c) The fundamental strength of the Waterfall Model has made it quite popular and handy among the fraternity. Major strengths are given as follows:

- It is ideal for supporting less experienced project teams and project managers or project teams, whose composition fluctuates.
- The orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.
- Progress of system development is measurable.
- It enables to conserve resources.

6. (a) Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. There should be enough information assembled so that a qualified person can understand the present system without visiting any of the operating departments. Survey of existing methods, procedures, data flow, outputs, files, input and internal controls that should be intensive to fully understand the present system and its related problems. The following areas should be studied in depth:

- **Reviewing Historical Aspects:** A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts enable to identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate 'what system changes have occurred in the past including operations' that have been successful or unsuccessful with computer equipment and techniques.
- **Analyzing 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 various sources from where the data are 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.
- **Reviewing Data Files:** The analyst should investigate the data files maintained by each department, 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 on-line and off-line files, which are maintained in the organization as it will reveal information about data that are not contained in any outputs. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.
- **Reviewing 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 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 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.

- **Analyzing 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 is used, how long is it kept on file, etc. must be investigated. Often, many reports are a carry-over from earlier days and have little relevance to current operations. Attempts should be made to eliminate all such reports in the new system.
- **Reviewing Internal Controls:** A detailed investigation of the present information system is not complete until internal control mechanism is 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 controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipments might allow much greater control over the data.
- **Modeling the Existing System:** As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the processes must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps to disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.
- **Undertaking Overall Analysis of the Existing 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; the present costs-benefits of each of these must be investigated thoroughly.

(b) Information Technology (IT) Governance: IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT. The objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT.

Benefits of IT Governance are as follows:

The benefits, which are achieved by implementing/improving governance or management of enterprise, IT would depend on the specific and unique environment of every enterprise. At the highest level, these could include:

- Increased value delivered through enterprise IT;
- Increased user satisfaction with IT services;
- Improved agility in supporting business needs;
- Better cost performance of IT;
- Improved management and mitigation of IT-related business risk;
- IT becoming an enabler for change rather than an inhibitor;
- Improved transparency and understanding of IT's contribution to the business;

- Improved compliance with relevant laws, regulations and policies; and
- More optimal utilization of IT resources.

(c) The requirements of Insurance Regulatory and Development Authority of India (IRDA) for System Controls are as follows:

- There should be Electronic transfer of Data without manual intervention. All Systems should be seamlessly integrated. Audit Trail required at every Data entry point. Procedures for reviewing and maintaining audit trail should be implemented.
- The auditor should comment on the audit trail maintained in the system for various activities. The auditor should review the Front Office Systems (FOS), MOS (Mid Office Systems) and BOS (Back Office Systems) and confirm that the system maintains audit trail for data entry, authorization, cancellation and any subsequent modifications.
- Further, the auditor shall also ascertain that the system has separate logins for each user and maintains trail of every transaction with respect to login ID, date and time for each data entry, authorization and modifications.