Test Series: April, 2021

MOCK TEST PAPER II

FINAL (OLD) COURSE GROUP - II

PAPER - 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Answer Keys

Part I: MULTIPLE CHOICE QUESTIONS

1. **(a)** The Spiral model combines the advantages of top-down and bottom-up concepts and is intended for large and complicated projects.

2. **(b)** (i), (ii), (iii)

3. **(d)** Identifying the mission/business-critical functions

4. **(b)** A – (iii), B - (i), C – (ii)

5. **(d)** Quality Assurance Management Control

6. **(d)** As it is a regulator for the securities market in India, it is responsive to the needs of investors and market intermediaries.

7. **(b)** (i), (iii), (iv)

8. **(c)** To determine whether programmer employee automated facilities to assist them with their coding work or not.

9. **(d)** Can the proposed application be implemented with existing technology?

10. **(a)** Transaction Processing System under Operational Level Systems

11. **(b)** Piggybacking

12. **(b)** Incremental Backup

13. **(d)** Document Evaluation

14. **(d)** Presence of Network Access Controls in organization.

15. **(b)** imprisonment upto 3 years or with fine which may extend upto 2 lakh rupees or with both.

16. **(d)** Programming Languages

17. **(c)** COBIT 5 has total of 39 Governance and Management processes.

18. **(c)** Teleconferencing and Video Conferencing Systems

19. **(d)** Data Coding

20. **(b)** (iv) – (ii) – (i) – (iii)

21. **(c)** System Analyst

22. **(b)** System Control Audit Review File

Part-II: Descriptive Questions

1. **(a)** **Information Security Policy** is the statement of intent by the management about how to protect a company's information assets. It is a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide. In its basic form, a information security policy is a document that describes an organization's information security controls and activities. The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business.

An Information Security Policy is the essential foundation for an effective and comprehensive information security program. It is the primary way in which management's information security concerns are translated into specific measurable and testable goals and objectives. It provides guidance to the people, who build, install, and maintain information systems. Information Security policy invariably includes rules intended to:

- Preserve and protect information from any unauthorized modification, access or disclosure;
- Limit or eliminate potential legal liability from employees or third parties; and
- Prevent waste or inappropriate use of the resources of an organization.

An information security policy should be in written form. It provides instructions to employees about 'what kinds of behavior or resource usage are required and acceptable', and about 'what is unacceptable'. An Information Security policy also provides direction to all employees about how to protect organization's information assets, and instructions regarding acceptable (and unacceptable) practices and behavior.

Tools to Implement Policy: As policy is in the form of a broad general statement, organizations also develop standards, guidelines, and procedures that offer users, managers and others a clearer approach to implementing policy and meeting organizational goals.

Standards specify technologies and methodologies to be used to secure systems. Guidelines help in smooth implementation of information security policy. Procedures are more detailed steps to be followed to accomplish particular security related tasks. Standards, guidelines, and procedures should be promulgated throughout an organization through handbooks or manuals. Organizational standards specify uniform use of specific technologies across the organization. Standardization of organization-wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are compulsory within an organization. Guidelines assist users, systems personnel, and others in effectively securing their systems. Guidelines are often used to ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.

An Information Security policy addresses many issues such as confidentiality, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

Issues to address: This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following 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.

Members of Security Policy: Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the three groups of management: Management members who have budget and policy authority, Technical group who know what can and cannot be supported, and Legal experts who know the legal ramifications of various policy charges.

(b) The key functions of the IT Steering Committee would include the following:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

(c) **Inherent Risk** is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same.

Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.

2. **(a)** Audit Trails under Programming Management Controls are as follows:

Phase	Audit Trails
Planning	• They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired. • They must evaluate how well the planning work is being undertaken.
Control	• They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. • They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample if past and current software development and acquisition projects carried out at different locations in the organization they are auditing.
Design	• Auditors should find out whether programmers use some type of systematic approach to design. • Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.

Coding	• Auditors should seek evidence – o On the level of care exercised by programming management in choosing a module implementation and integration strategy. o To determine whether programming management ensures that programmers follow structured programming conventions. o To check whether programmers employ automated facilities to assist them with their coding work.
Testing	• Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. • Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. • Auditors primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Maintenance	• Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. • Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

(b) **Business Impact Analysis (BIA)** is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. The process of BIA determines and documents the impact of a disruption of the activities that support its key products and services. 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. For each activity supporting the delivery of key products and services within the scope of its BCM program, the enterprise should:

- assess the impacts that would occur if the activity was disrupted over a period of time;
- identify the maximum time period after the start of a disruption within which the activity needs to be resumed;
- Identify critical business processes;
- assess the minimum level at which the activity needs to be performed on its resumption;
- identify the length of time within which normal levels of operation need to be resumed; and
- Identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

The enterprise should have a documented approach to conduct BIA. The enterprise should document its approach to assessing the impact of disruption and its findings and conclusions. The BIA Report should be presented to the Top Management .This report identifies critical service functions and the time frame in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities. Developing the BCP also takes into account the BIA process.

(c) Physical Component Controls: These controls incorporate features that mitigate the possible effects of exposures. The following table gives an overview of how physical components can affect communication subsystem reliability.

Transmission Media	It is a physical path along which a signal can be transmitted between a sender and a receiver. It is of two types: • **Guided/Bound Media** in which the signals are transported along an enclosed physical path like – Twisted pair, coaxial cable, and optical fiber. • In **Unguided Media**, the signals propagate via free-space emission like – satellite microwave, radio frequency and infrared.
Communication Lines	The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.
Modem	• Increases the speed with which data can be transmitted over a communication line. • Reduces the number of line errors that arise through distortion if they use a process called equalization. • Reduces the number of line errors that arise through noise.
Port Protection Devices	• Used to mitigate exposures associated with dial-up access to a computer system. The port-protection device performs various security functions to authenticate users.
Multiplexers and Concentrators	• These allow the band width or capacity of a communication line to be used more effectively. • These share the use of a high-cost transmission line among many messages that arrive at the multiplexer or concentration point from multiple low cost source lines.

3. (a) Major characteristics of an effective Management Information System are given as follows:

- **Management Oriented –** It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management as well.
- **Management Directed –** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- **Integrated –** The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.
- **Common Data Flows –** It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This

eliminates duplication in data collections, simplifies operations and produces an efficient information system.

- **Heavy Planning Element –** An MIS usually takes one to three years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
- **Sub System Concept –** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time by developing a phased plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- **Common Database –** Database is the mortar that holds the functional systems together. It is defined as a "super-file", which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
- **Computerized -** Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

(b) An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

- Analysis of business processes and level of automation,
- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,
- Studying network diagrams to understand physical and logical network connectivity,
- Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,
- And finally, Studying Information Technology policies, standards, guidelines and procedures.

(c) (i) "**Computer**" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

(ii) "**Addressee**" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

4. (a) This is **Hybrid Cloud** which 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 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.

The limitation of Hybrid Cloud is that the security features are not as good as the public cloud and complex to manage.

(b) Segregation of Duties: Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose is to prevent or detect errors or irregularities by applying suitable controls. It reduces the likelihood of errors and wrongful acts going undetected because the activities of one group or individual will serve as a check on the activities of the other. The irregularities are frauds due to various facts like Theft of assets like funds, IT equipment, the data and programs; Modification of the data leading to misstated and inaccurate financial statements; and Modification of programs in order to perpetrate irregularities like rounding down, salami etc.

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. However, in a computerized system, the critical factors that need to be considered are Nature of business operations; Managerial policy; Organization structure with job description; and IT resources deployed such as Operating system, Networking, Database, Application software, Technical staff available, IT services provided in-house or outsourced, Centralized or decentralized IT operations.

Examples of Segregation of Duties are as follows:

- Systems software programming group from the application programming group;
- Database administration group from other data processing activities;
- Computer hardware operations from the other groups;

- Systems analyst function from the programming function;
- Physical, data, and online security group(s) from the other IS functions; and
- IS Audit from business operations groups.

(c) 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.

5. (a) Mr. Y can be convicted and sentenced under **Section 67** of Information Technology Act, 2000. The detail of section is as follows:

[Section 67] Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

(b) The categories of Information Systems Audit are as follows:

(i) **Systems and Applications:** 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) Management should establish acquisition standards that address the security and reliability issues as per current state-of-the art development standards. Acquisition standards should focus on the following:

- ❖ Ensuring security, reliability, and functionality already built into a product;
- ❖ Ensuring managers complete appropriate vendor, contract, and licensing reviews and acquiring products compatible with existing systems;
- ❖ Invitations-to-tender soliciting bids from vendors when acquiring hardware or integrated systems of hardware and software;

- ❖ Request-for-proposals soliciting bids when acquiring off-the-shelf or third-party developed software; and
- ❖ Establishing acquisition standards to ensure functional, security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.

6. (a) The generic key aspects involved in System Development phase include the following:

(i) Program Coding Standards: The logic of the program outlined in the flowcharts is converted into program statements or instructions at this stage. For each language, there are specific rules concerning format and syntax. Syntax means vocabulary, punctuation and grammatical rules available in the language manuals that the programmer has to follow strictly and pedantically. Different programmers may write a program using different sets of instructions but each giving the same results. Therefore, the coding standards are defined, which serves as a method of communication between teams, amongst the team members and users, thus working as a good control. Coding standards minimize the system development setbacks due to programmer turnover. Coding standards provide simplicity, interoperability, compatibility, efficient utilization of resources and least processing time.

(ii) Programming Language: Application programs are coded in the form of statements or instructions and the same is converted by the compiler to object code for the computer to understand and execute. The programming languages commonly used are given as follows:

- High level general purpose programming languages such as COBOL and C;
- Object oriented languages such as C++, JAVA etc.;
- Scripting language such as JAVAScript, VBScript; and
- Decision Support or Logic Programming languages such as LISP and PROLOG.

The choice of a programming language may depend on various pertinent parameters. In general, language selection may be made on the basis of application area; algorithmic complexity; environment in which software has to be executed; performance consideration; data structure complexity; knowledge of software development staff; and capability of in-house staff for maintenance.

(iii) Program Debugging: Debugging is the most primitive form of testing activity, which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by the programmer into machine language instructions. Debugging can be a tedious task consisting of following four steps:

- Giving input the source program to the compiler,
- Letting the compiler to find errors in the program,
- Correcting lines of code that are erroneous, and
- Resubmitting the corrected source program as input to the compiler.

(iv) Testing the Programs: A careful and thorough testing of each program is imperative to the successful installation of any system. The programmer should plan the testing to be performed, including testing of all the possible exceptions. The test plan should require the execution of all standard processing logic based on chosen testing strategy/techniques. The program test plan should be discussed with the project manager and/or system users. A log of test results and all conditions successfully tested should be kept. The log will prove invaluable in finding the faults and debugging.

(v) Program Documentation: The writing of narrative procedures and instructions for people, who will use software is done throughout the program life cycle. Managers and users should

carefully review both internal and external documentation in order to ensure that the software and system behave as the documentation indicates. If they do not, documentation should be revised. User documentation should also be reviewed for understandability i.e. the documentation should be prepared in such a way that the user can clearly understand the instructions.

(vi) Program Maintenance: The requirements of business data processing applications are subject to periodic change. This calls for modification of various programs. There are usually separate categories of programmers called maintenance programmers, who are entrusted with this task.

(b) 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. The corporate governance is monitored by the audit committee.

Business Governance: The Business Governance is business-oriented with pro-active and forward-looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required. The business governance in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee.

(c) [Section 15] Secure Electronic Signature

An electronic signature shall be deemed to be a secure electronic signature if-

(i) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation – In case of Digital signature, the "signature creation data" means the private key of the subscriber.