It Covers
> ICAI Study Material
> ICAI Practice Manual
> Solved Question Papers of Last 35 Exams & Practice Manual
> Upto date Amendments Including CARO 2015 & Format of New Audit Report Under Companies Act, 2013.

3rd Edition

A COMPLETE GUIDE FOR ADVANCED AUDITING

(CA FINAL)

Applicable for CA Final May, 2016 & November, 2016 Exams onwards

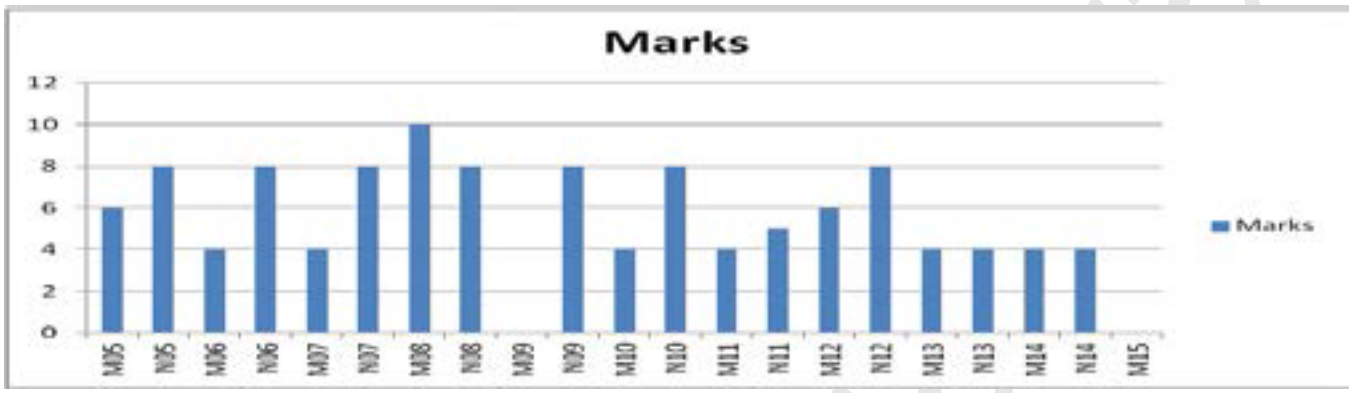
Short Notes for Quick Revision

CA is now Easy with Easy Ca™

Advanced Auditing and Professional Ethics

CA Sumit Aggarwal

5 AUDIT UNDER COMPUTERISED INFORMATION SYSTEM (CIS) ENVIROMENT



1. **Introduction:** Now-a-days, the corporate world is getting more and more inclined towards the use of Information technology (IT) and computer information system (CIS) in their daily operations. This has changed the manner in which the organisations' carry out their operations and various business processes. This has further led to change in the nature of audit evidences generated by each financial transaction and method of collection and evaluation of audit evidences by the auditor. Now, it is very important for the auditor to know about the current IT trend and its impact on auditing.

2. **Scope of Audit in a CIS Environment:** The use of CIS in various organisations has caused drastic impact on audit approaches, techniques, risk involved and internal control procedures. Following factors must be given due consideration while framing an audit plan for an organisation:
   - **High speed and Automatic Initiation/Execution of Transactions:** In CIS environment, transactions are processed instantly. Similarly, reports (even complex one's also) can be generated at a very high speed and can be viewed by multiple users at a time. Thus giving rise to many security issues.
   - **Uniform Processing of transaction, hence low clerical error:,** Computer system performs multiple checks on data, while feeding input, processing transactions and generating outputs. Moreover, the processing of transaction is in a uniform manner. Hence the clerical errors generated are minimised.
   - **Inexperienced Personnel:** Now-a-days, the technological advancement is occurring at a very fast pace. It has created a deficit of expertized staff to understand the current technology, both at client end as well as auditor end.
   - **Concentration of Duties** - In a manual environment the auditor needs to deploy separate individuals for carrying out the verification process. In a CIS environment, the traditional approach does not apply in many cases, as computer programs perform more than one set of activities at a time. This leads to difficulty in segregation of duties among individual. Consequently, it gives rise to a number of security issues also.
   - **Disappearance of Manual Reasonableness** - The shift from traditional manual information processing environment to CIS environment needs a detailed analysis of the physical system for transformation into a logical platform. In creating such logical models many stages required under manual operations are either deleted or managed to create a focused computer system. In such creative effort, the manual reasonableness may be missing.
   - **Impact of Poor System** - If system analysis and designs, falls short of expected standard of performance, a CIS environment may do more harm to integrated business operation than good. Thus, care has to be taken in adopting manual operations switch-over to computerised operations for ensuring performance quality standards.

3 **Impact of Changes on Business Processes (shifting from Manual to Electronic Medium):**
   - **EDI:** Electronic Data Inter-change, as the name suggests means exchange of data/information from one user to another, electronically (with the help of computers). In other words, EDI is the computer-to-computer exchange of documents/information in public standard format. Under EDI framework, once transaction (data) is fed into a computer many records are automatically updated. There is no need to

re-enter the data into accounting system. This saves a lot of time & effort and enables an error free transaction processing system (TPS).

- **Process of Recording Transactions: Unlike,** manual system where a transaction goes through a sequence of steps in order to get recorded in the principal books [Entry Ledger, Journal ledger, Final Accounts (Balance Sheet and P & L A/c)]. Under CIS environment, the above mentioned three processes are carried out simultaneously.
- **Accounting / Transaction Processing System:** As mentioned above the CIS mechanism leads to abandonment of maintenance primary records.

4. Recent changes in IT Environment, which may need to be addressed by the auditor in discharging their responsibilities in such IT environment:

- Mainframes are substituted by mini/micro users.
- There is a shift from proprietary operating system to more universal ones like UNIX, LINUX, Programming in 'C' etc (Single user to multi user).
- Relational Data Base Management system (RDBMS) are increasingly being used.
- The methodology adopted for systems development is becoming crucial and CASE (Computer Aided Software Engineering) tools are being used by many organisation.
- End user computing is on the increase resulting in decentralized data processing.
- The need for data communication and networking is increasing.
- Common business documents are getting replaced by paperless electronic data interface (EDI).
- Conventional data entry giving way to scanner, digitized image processes, voice recognition system etc.

The Impact of all such change on auditing may be summarised as:

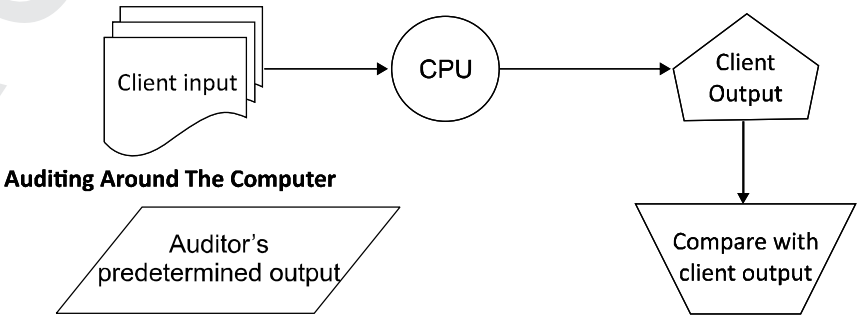
- Wide-spread end-user computing may result in unintentional errors.
- Usage of sophisticated audit software would be a necessity.
- Auditors non-participation at System Development Life Cycle State (SDLC) pose considerable problem in understanding the operational controls.
- Data communication and net working would introduce new audit risk.
- The move toward paperless EDI would eliminate much of the traditional audit trail radically changing the nature of audit trails.

5. Audit Approach in a CIS Environment: Based on the knowledge and expertise of Auditors in handling computerised data, the audit approach in a CIS environment could be either:

- A Black-box approach i.e., Auditing around the computer, or
- A White-box approach i.e., Auditing through the computer.

5.1 The Black Box Approach (Auditing Around the Computer): In the Black box approach, the Auditor concentrates on input and output and ignores the specifics of how computer process the data or transactions. If input matches the output, the auditor assumes that the processing of transaction/data must have been correct. For example, while testing payroll of a company, under black-box approach, the auditor may first find out the total monthly hours worked by selected employees from their respective time cards and then he may check the salary/wage rate from the rate card to find out the salary/wage payable to each employee. On the basis of above, the auditor ascertains his own output by comparing hours, rates, extensions, over-time & leaves. Finally, the auditor compares his own results with the system generated results.This approach may be enumerated with the help of the following flowchart:

A. The Black Box Approach

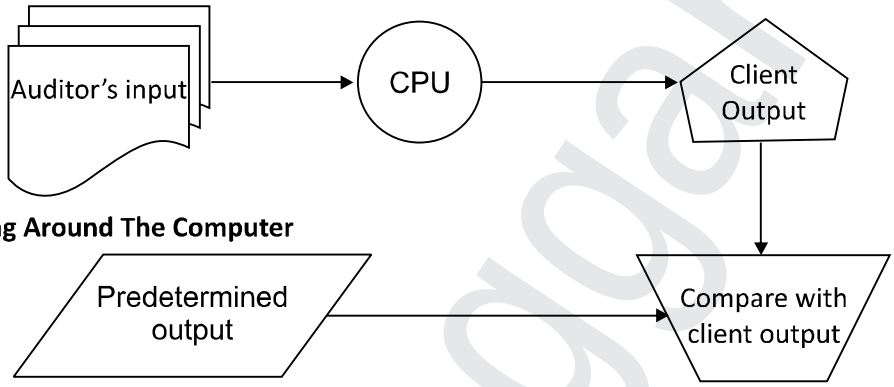


The biggest advantage of auditing around the computer is the ease and simplicity, since the auditor does not require in-depth knowledge of system application program in order to perform his duties.

On the contrary, a major disadvantage is that, under this approach, the auditor is completely ignorant about the internal processes of the system. Moreover, in order to generate certain complex reports, print-outs cannot be arranged to apply the audit procedures.

5.2 White-Box Approach (Auditing Through the Computer): Under this approach, the auditor is not only concerned with the subject matter of the audit (i.e. inputs and outputs), but also with the internal processing of the computer system. This means to include various auditing technique with the help of Audit software and computer aided audit techniques (CAAT). This can be explained with the help of following flowchart:

B. The White Box Approach



Auditing Around The Computer

6. Types of Computer Systems: There is large variety of computer systems applicable to accounting and other type of information processing. The nature and type of system affect the various types of controls. Computer System may be broadly classified as under:

- Based on System configuration, and
- Based on Processing systems.

6.1. Based on Systems Configuration: System configuration may be classified as:

- **Large System Computers:** In large system computers, the processing task of multiple users is performed on a single centralised computer, i.e., all inputs move directly from the terminal to central processors and after processing goes back to users from central processors. All the terminals in these systems were called 'dumb terminals' as these terminals were not capable of processing data on their own and casually serve only as input/output terminals.
- **Stand Alone Personal Computers:** A stand alone system is one that is not connected to or does not communicate with another computer system. All input data and its processing takes place on the machine itself. Many small businesses rely on personal computers for all their accounting functions.
- **Network Computing System:** A network is a group of interconnected system sharing services and interacting by a shared communication links. All networks have something to share, a transmission medium and rules for communication. Network share hardware and software resources.
- **Electronic Data Interchange (EDI)** - The transfer of electronic data from one organisations computer system to another's, the data being structured in a commonly agreed format so that it is directly usable by the receiving organisation computer system. EDI may be introduced where a group of organisations wish to ensure that electronic transactions are passed between one another. The following benefits accrue under EDI systems.
  - ◊ The speed with which an inter-organisational transaction is processed is minimised.
  - ◊ The paperwork involved in transaction processing is eliminated.
  - ◊ The costs of transaction processing are reduced, as much of the need for human interpretation and processing is removed.
  - ◊ Reduced human involvement reduces error.

6.2. Based on Processing system:

No.	Batch Processing (Old Concept	On Line Procressing System/ On Line Read time processing	Time Sharing & Service Bureau (Distinct & New Concept)
1	In this process transactions are accumulated and processed in groups.	Under this system transaction are processed as soon as they occur.	Time sharing is a situation where a single computer serves more than one user.
2	In this files are not updated quickly.	All the records are updated simultaneously on occurrence of a transaction.	A service bureau is an entity that proceses transactions for other entities. For Example service bureau may handle the complete payroll processing for small companies.
3	Example: Accountant accumulates all the cash receipts vouchers for the day and updates his accounting record by the end of a working day.	E.g.: On issue of a Sales invoice, Sales ledger and debtor's ledger are updated, automatically.	If an organisation uses services of a service bureau, then the auditor must obtain reasonable evidences in support of the controls exercised by the client organisation over the activities performed by service bureau.
4	This is simple system, but now a days rarely found due to availability of advanced and quick systems.	Software packages ,like Tally, SAP, etc. works like this.	Nowadays, many of accounting firms are doing this kind of activities.

7. **Problems that may arise in the implementation of Internal Control in EDP system [N02 N04]:** Internal control system include separation of duties, delegation of authority and responsibility, a system of authorisation, adequate documents and records, physical control over assets and records, management supervision etc. In CIS environment, all these components must exist but computers affects the implementation of these internal controls in many ways. Some of the effects are as under:
   - **Separation of Duties** - In a manual system, different persons are responsible for carrying out different function like initiating, recording of transaction, custody of assets etc. Due to automation in the system, such controls are not possible in a computer system.
   - **Delegation of Authority and Responsibility** - A structured authority and responsibility is an essential control within manual and computer environment. In a computer system however, a clean line of authority and responsibility might be difficult to establish because some resources (database etc) are used by multiple users.
   - **Competent And Trustworthy Personnel:** Skilled, competent, well-trained and experienced information system personnel have been in short supply. Organization finds it difficult to find and retain competent and trustworthy personnel to take charge their EDP setup.
   - **System of Authorisation:** As against the manual system, automation of the authorization procedures is an important feature of EDP System. In a computer system, it is difficult for the auditor to assess, whether the authority assigned to individual persons is constant with managements policies. For example, the computer system may determine the price to be charged to customers. Thus, in evaluating the adequacy of authorisation procedures, auditors have to examine not only the work of employees but also the veracity of the programme processing.
   - **Adequate Documents and Records:** In computer system, document support might not be necessary to initiate, execute and records some transaction. Thus, no visible audit trail may be available. This creates a serious control problem.
   - **Physical Control over Assets and Records:** Physical access to assets and records is critical in both manual systems and computer system. In a computer system the information system assets and records may be concentrated at a single site. The risk of loss and unauthorized access is high.
   - **Adequate Management Supervision:** In a computer system, supervision of employee might have to be carried out remotely, because in IT environment employees are closer to the customer to whom they provide services.

- **Independent Checks On Performance:** Checks by an independent person help to detect any errors or irregularities.
- **Comparing Recorded Accountability with Assets:** In a manual system, independent staff prepares the basic data used for comparison purposes. But in a computer system, records may be automatically reconciled with assets. Thus unauthorized modification to programs or data files that these programs use, may be difficult to detect. Therefore care must be taken, that there is no unauthorized modifications to this programs or to any of the data files, otherwise the irregularity may not be discovered.

8. Review of Checks & Type of Internal Controls in EDP/CIS Environment: An internal control in an EDP environment depends on the same principal as that of manual system. However, in a CIS environment, due to difference in approach there is various other types of controls which operate over data input, processing & output of CIS. These are designed in such a way that the correct, complete and reliable processing and storage is ensured. It is necessary for the auditor to review such controls in order to get the correct result from the data entered. Generally there is two type of control in EDP environment:

- General control affecting EDP environment.
- Specific controls over specific application.

9. General EDP Controls:

9.1. Organization Structure and Management Control: The entity may have different functions under the CIS environment such as:

- Data base administrators who will formulate data policies, plans the evaluation of the corporate data bases and maintain the data documentation. He is responsible for operational efficiency of the database.
- The system Analyst will manage the information requirements for new and existing applications, and designs the information system.
- The System programmer will maintain and enhance the Operating system software. Application programmer will design the programme to meet the information requirement.
- Operation Specialist plans and control day-to-day operations, monitors and improves operational efficiency along with capacity planning.
- Librarian maintains library of magnetic media and documentation.

The auditor will see that the responsibilities of each job position are clear and that the person understands the duties, authority and responsibilities. The duties have to be separated to ensure the internal control is established.

9.2 System Software Controls: Restricted access of software to authrosied personnel only.

9.3 Application System Development and Maintenance Controls [N99]: System development controls are necessary to ensure that a computer based system operates as originally envisaged and the relevant documents have been properly prepared and maintained. The main requirements and techniques of systems development controls are considered below:-

- Restricted access to documentation related system development.
- Changes to application systems should be authorized.
- Testing and implementation of the new systems in a proper way.
- Acquisition of application system from third parties should be carefully planned.

9.4 Computer Operation Controls:

- Only authorized person should have access to the computers.
- The system is used for authorized purpose only.
- Only authorized programs/software to be used.
- Processing error are detected and corrected on a timely basis.

9.5 Data Entry and Program Controls:

- Access to data and program is restricted to authorized personnel.
- An authorisation structure is established over transaction being entered into the system.

9.6 Documentation Control: The auditor has to see that there is proper and adequate documentation for approval of system flowcharts Programme flowcharts, Programme changes, operator's instructions and programme description and the changes made in the above are also documented and approved by the

authorized persons.

9.7 **Access Control:** The auditor has to ensure that, the system prevents the persons who are authorized for access from accessing restricted data and programme and also prevents unauthorized persons gaining access to the system as a whole.

9.8 **Recording Controls:** The auditor has to ensure that records to be kept free of errors.

9.9 **Storage Controls:** The auditor has to ensure that backup and recovery facilities will ensure the proper data availability to the management.

10 Specific Controls over Specific Application (Application Control) [N98 N10 N13]:

10.1 **Controls over Input:** To check whether:

- Input Data is duly authorized and accurate before being processed by the computer.
- For validation of input controls the auditor can apply some procedures like Check digit control, completeness totals control, reasonableness checks, field checks, record checks, file checks etc.
- Transaction are accurately converted into machine readable form and recorded in the computer files.
- Transaction are not lost, added, duplicated or improperly changed.
- Incorrect transactions are rejected or re-submitted after correction.

10.2 **Controls over Processing and Computer data files:** To check whether:

- Processing errors are detected and corrected on a timely basis.
- Transactions are properly processed by the computers.
- Processing validation checks should be applied to ensure processing controls.

10.3 **Controls over Output:** To check whether:

- Output is complete and accurate.
- Access to output is restricted to authorized personnel.
- Output so generated; satisfy the requirement of the user.
- Output is provided to appropriate authorized personnel on timely basis.
- The audit trail relating to output is provided.

11. Nature of risk and the Internal Control characteristics in CIS environment [N05]:

- **Lack of Transaction Trails:** All CIS do not provide complete audit trail. Hence, where audit trail is not available, audit risk will be high.
- **Uniform Processing of Transactions:** Computer process uniformly all the transactions with the same processing instructions. Hence there is no clerical error in Computer programs, but programming error may occur.
- **Lack of Segregation of Functions:** Many control procedures that would ordinarily be performed by separate individuals in manual systems, may become concentrated in a CIS environment i.e. Extent of segregation is limited in CIS environment as compared to manual systems. Thus, an individual who has access to computer programs, processing or data may be in a position to perform incompatible functions.
- **Potential for Errors and Irregularities:** Due to technical incompetence, the potential for human error in the development, maintenance and execution of CIS may be greater than in manual systems.
- **Automatic Execution of Transactions:** CIS execute certain types of transactions automatically. The authorization of these transactions may not be documented.
- **Dependence of Other Controls over Computer Processing:** Computer processing may produce reports and other output that are used in performing manual control procedures. The effectiveness of these manual control procedures can be dependent on the effectiveness of controls over the completeness and accuracy of computer processing.
- **Increased Management Supervision:** Computer information can offer management a variety of analytical tools that may be used by the management to review and supervise the operations of the entity. The availability of these analytical tools, if used, will enhance the effectiveness of the entire internal control structure.
- **Use of Computer - Assisted Audit Techniques (CAAT):** In CIS environment, where large quantity of data is processed by CIS, the Auditor may apply general or specialized computer audit techniques and tools in the execution of audit tests.

12. **Specific Risk related to an Entity's Internal Control [M10]:** As per SA 315 "Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and its Environment", IT system also poses some specific risks to an entity's Internal Control. They are given below:
    - Reliance on systems or programs that are inaccurately processing data, processing inaccurate data or both.
    - Unauthorised access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions, or inaccurate recording of transactions. Particular risk may arise when multiple users access a common database.
    - The possibility of IT personnel gaining access beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.
    - Unauthorised changes to systems or programs.
    - Unauthorised changes to data in Master files.
    - Failure to make necessary changes to systems or programs.
    - In appropriate manual intervention.
    - Potential loss of data or inability to access data as required.

13. **A Causes of Risk of Material Misstatement in CIS Environment [M14]:** In a CIS environment cause of risk of material misstatement may arise in the following cases:
    - Program Development and maintenance.
    - System software support.
    - Operations including processing of data.
    - Physical CIS security.
    - Control over access to specialized utility program.

14. **Factors to be consider while evaluating the reliability of the Accounting and Internal Control Systems in CIS Environment [N08 N12] :** While evaluating the reliability of the accounting and internal control systems, the auditor would consider whether these systems:
    - **Authenticity Control:** Ensure that authorized, correct and complete data is made available for processing. (Password, digital signature etc.)
    - **Accuracy Control:** Ensure that detection and correction of errors done on timely basis (Programme, Validation Check).
    - **Redundancy Control:** ensures that processing of data is done only once.
    - **Audit Trail Control:** This ensures the traceability of all events occurred in a system.
    - **Backup Control:** Ensure that proper backup system is available in case of interruption due to power, mechanical or processing failures.
    - **Completeness Control:** Ensure that output is correct and complete.
    - **Existence Control:** It attempts to ensure the ongoing availability of all system resources.
    - **Asset Safeguarding Controls:** It attempts to ensure that all resources within a system are protected from destruction or corruption such fire, wrong processing frauds etc.
    - Ensure that **amendments to the programs** are properly authorized.
    - Ensure **safe custody of source code** of application software and data files.
    - **Effectiveness Control:** It attempts to ensure that the system achieves its goals.
    - **Efficiency Control:** It attempts to ensure that a system uses minimum resources to achieve its goals.

15. **Effects of Computers on Auditing [N07 N09 N14]:** The objective of auditing, do not change, when auditor performs audit in a CIS environment. However, computer systems have affected how auditors need to collect and evaluate evidence. These aspects are discussed below:

15.1 **Changes to Evidence Collection:** Collecting evidence on the reliability of a computer system is often more complex than collecting evidence on the reliability of a manual system. Auditors have to face a diverse and complex range of internal control technology that did not exist in manual system, for example:
    - Accurate and complete operations of a disk drive may require a set of hardware controls not required in manual system.
    - System development control includes procedures for testing programs that again are not necessary in manual control.

    Auditors must understand these controls to collect evidence competently on the reliability of the controls.

Unfortunately, understanding the changing technology is also not easy. Rapid development in hardware and software is continuing, the associated control is also developing rapidly. Auditors must keep up to-date with the developments to evaluate the reliability of accounting system.

The continuing development of computer technology also makes it more difficult for auditors to collect evidence on the reliability of controls. It may be impossible for auditors to obtain the evidence using manual means. Thus auditors also need EDP systems to collect the necessary evidence. The development of generalised audit software occurred, for example, because auditors needed access to data maintained on magnetic media. Similarly, new audit tools may be required, in due course, to evaluate the controls.

15.2 Changes to Evidence Evaluation: With increasing complexity of computer systems and control technology, it is becoming more and more difficult for the auditors to evaluate the consequences of strength and weaknesses of control mechanism, for placing overall reliability on the system.

16. Auditing approach in a CIS Environment: The overall objective and scope of an audit do not change in a CIS environment. However, the use a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the entity. The auditor should consider the effect of the factor like,

- The extent of use of computers for preparing accounting information.
- Efficacy of internal control over input, processing, analysis and reporting, undertaken in the CIS installation and
- The impact of computerisation on the audit trail that could otherwise be expected to exist in a manual system.

17. Perquisites while Auditing in CIS Environment:

- **Knowledge of Business:** An auditor should have sufficient knowledge of the CIS to plan, direct, supervise control and review the work performed. The sufficiency of knowledge would depend on the nature and extent of the CIS environment.
- **Skill and Competence:** The auditor should consider whether any specialized CIS skills are needed in the conduct of the audit. If the answer is yes, he may seek the assistance of an expert possessing such skills.
- **Planning:** To plan the audit and to determine the NTE of the audit procedures, the auditor should have understanding of the following:
  - ◊ The CIS infrastructure (hardware, operating system (s) and application software used by the entity, including changes therein since last audit, if any)
  - ◊ The significance and complexity of computerized processing.
  - ◊ Availability of data by reference to source documents, computer files and other evidential matters.
- **Assessment of Risk:** The auditor should assess, whether CIS environment may influence the assessment of inherent and control risks.

18. Computer Assisted Audit Techniques (CAATS) [M00]: The overall objectives and scope of an audit do not change when an audit is conducted in a (CIS) environment. The application of auditing procedures may, however, require the auditor to consider techniques known as Computer Assisted Audit Techniques (CAATs) that use the computer as an audit tool for enhancing the effectiveness and efficiency of audit procedures. CAATs are computer programs and data that the auditor uses as part of the audit procedures to process data of audit significance, contained in an entity's information systems. The use of CAAT may be required because of following reasons:

- **Internal Storage:** Internal storage is a representation of the information in electronic form inside the computer. As a result of this, the auditor is unable to observe the processing of data to determine whether procedures are being followed.
- **Visual Observation:** Visual observation is more difficult because of the speed with which the equipment operates. Even slowing down the system may be of no value to the auditor because of his inability to understand the electronic pulses or information stored in an electronic media.
- **Disappearance of Audit Trail:** Audit trail can be explained as those documents, records, journals ledgers, master files etc, that enables an auditor to trace the transactions from the source document to the summarized total in accounting reports or vice versa. In a computerised environment where the data are being entered directly into the system the auditor faces the problem of partial elimination or disappearance of audit trail.

- **Ease of access to Data and Computer Program:** Data and computer programs may be accessed and altered at the computer or through the use of computer equipment at remote location. Therefore, in the absence of appropriate controls, there is an increased potential for unauthorized access to and alteration of data and programs by persons inside or outside the entity.
- **CAATs can be used for both Compliance and Substantive Procedures, including the following:**
  - ◊ Tests of details of transactions and balances.
  - ◊ Analytical procedures.
  - ◊ Testing aging analysis of debtors, inventory etc.
  - ◊ Compliance tests of general EDP controls and application controls.

Thus, while planning an audit, the auditor may consider an appropriate combination of manual and CAATs. The most common types of CAATs used for audit purposes are.

- **Audit Software:** It consists of computer program used by the auditor as a part of his procedure to process data of audit significance.
- **Test Data:** These are used in conducting audit procedures by entering data into computer system and comparing data with predetermined results.

19. **Audit Procedure using CAATs [M12 M13] :** CAATs allow the auditor to (a) give access to data without dependence on the client, (b) test the reliability of client software, and perform audit tests more efficiently. CAAT are used to perform various auditing procedures like:
    - **Tests of Details of Transactions and Balances:** For example, the use of audit software for recalculating interest or the extraction of invoices over a certain value from computer records.
    - **Analytical Review Procedures:** For example: use of audit software to identify unusual fluctuations or unusual items.
    - **Tests of General IT controls:** For example: testing the set-up or configuration of the operating system or access procedures to the program libraries or by using code comparison software to check that, the version of the program in use is the same version approved by the management.
    - **Sampling Programs** to extract data for audit testing.
    - **Tests of Application Controls:** For example: testing the functioning of a programmed control; and Reperforming calculations performed by the entity's accounting systems.

20. **Detection of Fraud and Error [M08]:** The CAAT allows the auditor to plan and execute the audit work more effectively with the help of sophisticated audit software. But, under CIS environment, frauds are intentional and generally deep-laid. Moreover, there are chances that some frauds are highlighted, but there is no concrete evidence to prove the same. Thus it cannot be said that the auditing through the computer will increase the probability of detection of fraud.

21. **Factor to be consider in determining the Use of CAAT In EDP environment [M05 M07]:** In determining whether to use CAAT, the following factors should be considered:
    - **Computer Knowledge, Expertise and Experience of the Auditor:** The auditor and audit team should have sufficient skills and experience to handle the audit under CAAT.
    - **Availability of CAATS and Suitable Computer Facilities:** The auditor may plan to use other computer facilities when the use of CAATs on an entity's computer is uneconomical or impractical for example, because of an incompatibility between the auditor's package programme and entity's computer.
    - **Impracticability of Manual Tests due to lack of Evidence:** Many CIS perform tasks for which no hard copy evidence is available; therefore, it may be impracticable for the auditor to perform tests manually.
    - **Effectiveness and Efficiency:** With the help of CAAT, it is possible to test large number of transactions together with a better level of precision. This brings efficiency and effectiveness in performing the audit assignment.
    - **Timing:** Certain data are often kept for a short period and may not be available in machine-readable form by the time auditor wants them. Thus, the auditor will either need to make arrangements for retention of such files or alter the timing of his audit.
    - **Use of CAAT in small Organisations:** In small business organisation, use of CAAT might not be a cost-effective and viable alternative. This is because of two reasons, first the revenue per assignment is not very huge, and second the client entity might not have the appropriate technical infrastructure to run CAAT.

22. **Steps in Implementation of CAATs:** The major steps to be undertaken by the auditor in the application of

CAAT are to:

- Set the objective of CAAT application.
- Determine the content and accessibility of the entity's files.
- Identify the specific files or databases to be examined.
- Understand the relationship between the data tables, where a database is to be examined.
- Define the specific tests or procedures and related transactions and balances affected.
- Define the output requirements.
- Arrange with the user and IT departments, if appropriate, for copies of the relevant files or database tables to be made at the appropriate cut-off date and time.
- Identify the personnel who may participate in the design and application of CAAT.
- Refine the estimates of costs and benefits.
- Ensure that the use of CAAT is properly controlled.
- Arrange the administrative activities, including the necessary skills and computer facilities.
- Reconcile data to be used for CAAT with the accounting and other records.
- Execute CAAT application.
- Evaluate the results.
- Documentation, that CAATs to be used including objectives, high level flowcharts and run instructions; and
- Assess the effect of changes to the programs/system on the use of CAAT.

23. **Testing CAAT:** Before applying or relying on CAAT, the auditor must first obtain reasonable assurance of the integrity, reliability, usefulness, and security of CAAT through appropriate planning, design, testing, processing and review of documentation.

24. **Controlling CAAT Application [M02 N03]:** The success or failure of auditing with CAAT highly depends upon the degree of control exercised on the overall application of CAAT. The control over the CAAT applications can be of two types:

A. Procedures carried out by the Auditor to Control Audit Software Application:

- Participation in design and testing of CAAT.
- Checking the coding program.
- Review of operating system used by the client to check Compatibility of the audit software with the client's information system.
- Testing the software before running it on client's data.
- Testing the test results.
- Establish appropriate security measures to safeguard the integrity and confidentiality of client's data.
- Ensure proper vender support during audit.

B. Procedures carried out by the Auditor to Control over Test Data Application:

- Predicting the results of the test data and comparing it with the actual test data output.
- Control the sequence of submission of test data where it spans several processing cycles.
- Performing test runs containing small amounts of test data before submitting the main audit test data.
- Confirming that the current version of the programs was used to process test data.
- Ensure that the client entity used the same version of software throughout the audit period, on which the audit is being conducted.
- Make sure that dummy entries are deleted, which were fed in the system, while performing the audit.

When using a CAAT, the auditor may require the co-operation of the entity's staff, who have extensive knowledge of the computer installation. In such cases, auditor should have reasonable assurance that the entity's staff did not improperly influence the results of the CAAT. Finally, the standard of working papers and retention procedures for a CAAT should be consistent with that on the audit as a whole. It may be convenient to keep the technical papers relating to the use of the CAAT separate from the other audit working papers. The working papers should contain sufficient documentation to describe CAAT application.

25. **Audit Trail [M08]:** It can be defined as a step-by-step record by which a transaction can be traced. A proper audit trail ensures audit checking for proper processing and accumulation of data. The extent of audit trail available in manual system may not be available in CIS due to following reasons.

- Source documents once transcribed in machine readable form are not retained in a manner that permits

subsequent access.
- Master files may replace ledger summaries.
- Transaction listing is often not provided.
- Reports may be only on exceptions.

26. Methods to Compensate the Loss of Audit Trail: The auditor may apply one of the following methods to compensate the loss of audit trail:

26.1 Special/Exceptional Reports: The auditor may ask the client to arrange special reports and printouts. For example: sales orders for the month of December & March; purchase orders that have been short-closed by the purchase department.

26.2 Tagging and Tracing [N04]:
- It is a method of compensating the audit trail.
- It involves tagging the clients input data in such a way that only relevant data is highlighted on the screen, which needs to be verified by the auditor.
- For example: cash payments of more than Rs. 20,000/-; debtors outstanding for more than 3 months; purchase order pending for more than 30 days from expected delivery date; sales orders processed in excess of Rs. 1,00,000 etc.

26.3 Alternative Review Procedures (ARP): It means to include a number of methods to compensate audit trial, such as:
- **Auditors' Judgement:** budgeting the figures and comparing them with actual figures.
- **Ratio Analysis.** This implies calculating certain ratios on the basis of budgeted data or previous period's data or data from similar industries and comparing them with the actual data of the client organisation.
- **Testing on Total Basis:** if individual items can't be checked in detail then auditor may take totals of reasonable chunks of data and check accordingly.
- **Clerical Recreation:** Auditor may manually generate certain figures that have been generated by the system (automatically).

27. Special Audit Techniques: In the absence of audit trail, the auditor needs the assurance that the programmes are functioning correctly in respect of specific items by using special audit techniques. In the absence of input documents or lack of visible audit trail may require the use of CAATs in using the computer as an Audit tool. The effectiveness and efficiency of auditing procedures may enhance through the use of CAATs. Two common types of CAATs are in vogue, (a) Test packs or test data and (b) audit software or computer audit programmes. Normally special audit techniques may be used under the following circumstances.
- To ensure the correct functioning of important programme controls.
- To overcome losses of audit trail.
- To reduce audit costs or increase the efficiency of the audit.

28. Audit Software: It consists of computer programs used by the auditor as a part of his audit procedures to process data of audit significance. The most common types of CAATs used for audit purposes are discussed as follows:
- **Package Programs:** These are generalized computer programs designed to perform data processing functions, such as reading data, selecting and analyzing information, performing calculations, creating data files and reporting in a format specified by the auditor. MS-Excel can be the most common example for such programs.
- **Purpose-Written Programs:** This software's are used to perform audit tasks in specific circumstances. These packages are not available for sale in the open market. These programs may be developed by the auditor, the entity being audited or an outside programmer hired by the auditor.
- **Utility Programs:** These programs are used for performing common data processing functions, such as sorting, creating and printing files. Although, these are not specifically designed for the audit purposes and therefore may not contain features such as automatic record counts or control totals, but it can be extremely useful while performing the audit.
- **System Management Programs:** These are productive tools, meant to enhance the performance of the Operating System. However, these tools are not specifically meant for audit purposes. Disk Defragment, Task Manager, Task Scheduler, Disk Clean-up, etc. are some of the examples of system management software.

29. **Test Packs or Test Data [M06]:** Test data techniques are used in conducting audit procedures by entering data into the computer system of the organisation and comparing the results obtained with predetermined results when test data is processed with the organization's normal processing the auditor should ensure that the test transactions are subsequently eliminated from accounting records of the organisations.

30. **Characteristics of an Effective Computer Audit Program System [M04 N06]:** - Computer audit program developed for general purposes shall have to customize according to the needs of the organisation. However an examination of following features is necessary to ensure that it is effective:
    - **Simplicity:** The system should be simple to use and eliminate the need for remembering countless details normally required in writing or revising computer programs.
    - **Understandability:** The system should be understandable by the members of the audit staff, even those with little computer expertise. The capabilities of the system should be known and it should be easy to use. Coding forms provided should not be difficult to understand.
    - **Adaptability:** The system should be capable of writing computer audit programs for the various types of computers used in the company or expected to be acquired. Thus the package will be usable if the equipment is changed in the future.
    - **Vendor Technical Support:** In considering the types of package to be acquired, it is important that the vendor provides adequate support. This includes assisting in the initial installation and providing adequate documentation training to the audit staff.
    - **Statistical Sampling Capability:** Statistical sampling is an important Application in auditing, the package should be able to perform the various statistical routines this should include the selection of items on a random basis, determination of sample size, and evaluation of results at different confidence levels.
    - **Acceptability:** The system should be acceptable to both the auditors and to computer centers. For the auditors the programs should be easily carried to the site and practical to use. For the computer centre the programs should be compatible with the system and capable of minimum interference with normal routines.
    - **Processing Capabilities:** The package should be able to process many different types of application. For example, it should accept all common file media and process multiple file input. It should have the capability for extended data selection and stratification; it should have powerful, generalized audit commands.
    - **Report Writing:** The package should have a strong report writing function. This should include the ability to prepare multiple reports in a single program run and to generate flexible output report formats.

31. **Characteristics of On-line Computer System [N04]:** The particular characteristics of a specific On-line Computer System will depend on the design of that system. However the most significant characteristics of On-line Computer system are given below:
    - **Validation Checks:** When data are entered on-line, they are usually subject to immediate validation checks. Data failing this validation would not be accepted and a message may be displayed on the terminal screen, providing the user with the ability to correct the data and re-enter the valid data immediately. For example, if the user enters an invalid inventory part number, an error message will be displayed enabling user to re-enter a valid part number.
    - **On-Line Access:** Users may have on-line access to the Computer system that enables them to perform various functions e.g. Entering input data and to read, change or delete programs etc. Unlimited access to all of these functions in a particular application is undesirable, because it provides the user with the potential ability to make unauthorized changes to the data and programs. The extent of this access will depend upon such things as the design of the particular application and the implementation of software, designed to control access to the system.
    - **Transaction Trail:** An on-line computer system may be designed in a way that does not provide supporting documents for all transactions entered into the system. For e.g. Orders received by a telephone operator who enters them on-line without written purchase orders, and cash withdrawals through the use of automated teller machines. However, the system may provide details of the transactions on request or through the use of transaction logs or other means.
    - **Programmer Access:** Programmers may have on-line access to the system that enables them to develop new programs and modify existing programs. Unrestricted access provides the programmer with the potential to make unauthorised changes to programs and obtain unauthorised access to other parts of the system. The extent of this access depends on the requirements of the system.

No.	Question Bank	Exam	Marks	Refer Point/ Ans.
1	Discuss some problems that will be encountered in an EDP system in implementation of internal control.	N02 PM	10	7
2	State the specific problems, which may arise in the implementation of internal control in an EDP system.	N04	8	
3	Write short Notes on "Systems Development Control".	N99	4	9.3
4	Draw up a check list for evaluation of output controls on accounts maintained under ED.P. System.	N98	8	10
5	Different types of controls which operate over data moving into, through and out of the computer. Auditor is required to review such controls. Comment.	N10 PM	8	
6	Q Ltd. operates in an ERP environment. Its auditor requires your assistance on the aspects that are needed to be looked into in respect of control over input and output of transactions. Kindly help him.	N13	4	
7	Enumerate the risk and internal control characteristics in an audit conducted in Computer Information Systems (CIS) environment.	N05	8	11
8	IT systems also pose specific risks to an entity's internal control? What are those risks.	M10 PM	4	12
9	Write short notes on " Causes of risk of material misstatement in CIS environment".	M14	4	13
10	The auditor must evaluate major clauses of control used in a Computerized Information system to enhance its reliability. Comment.	N08 PM	8	14
11	What are the considerations which an auditor should consider while evaluating the reliability of the accounting and internal control systems in a CIS environment?	N12 PM	8	
12	The role of an auditor in collecting audit evidences under EDP system is more complex than under the manual system. Discuss.	N09 PM	8	15
13	"The method of collecting Audit evidence and evaluating the same changes drastically under EDP Auditing." Comment on the above.	N07 PM	8	
14	How would the method of collecting audit evidence relating to effectiveness of controls and evaluating the same change under a computerized environment?	N14	4	
15	Describe the role of Computer-assisted Audit Techniques in E.D.P. Environment.	M00	10	18
16	In the audit of K Ltd its auditor wants to use CAATs for performing various audit procedures. Guide him as to what procedures can be performed using CAATs.	M12 PM	6	19
17	E & Co, a firm of Chartered Accountants, requires your help in identifying the audit procedures that can be performed using CAATs. Please guide them.	M13 PM	4	
18	"Use of Audit Software would increase the probability of detecting frauds". Comment.	M08	6	19, 20
19	Factors to consider in determining the use of Computer Assisted Audit Techniques (CAATs).	M07	4	21
20	In determining whether to use Computer Assisted Auditing Techniques (CAATs), what are the factors that a Statutory Auditor has to consider?	M05 PM	6	
21	Indicate the control procedures which the auditor should adopt in applying CAAT (Computer Assisted Audit Technique) in an audit under EDP environment.	M02 N03 PM	8, 16	24
22	What is an Audit Trail?	M08	4	25

23	Explain: Tagging and Tracing.	N04	4	26.2
24	Write short notes on "Test Packs".	M06	4	29
25	What is an Audit Trail? Briefly describe the special audit techniques using the computer as an audit tool.	N00 PM	8	25, 27, 28, 29
26	State the important characteristics of an effective computer audit program system.	M04 N06 PM	8	30
27	What are the characteristics of 'On-line Computer System'?	N04 PM	4	31
28	"Where the Financial Accounting System has not been computerized, the auditor need not verify Computerized Management System".	M00 PM	8	Ans - 1
29	A limited company having turnover of approximately Rs.50 crore uses a tailor made accounting software package. In the said package, all transactions are recorded, processed and the final accounts generated from the system. The management tells you that in view of the voluminous nature of day books, there is no need to print them and that audit can be conducted on the computer itself. The management further assures you that any 'query based reports' as required can be generated and printed. As a statutory auditor of the company, enumerate the procedures you would adopt to conduct the audit.	M01 PM	16	Ans - 2
30	Z Ltd. has its entire operations including accounting computerized as the audit partner' you are concerned about inherent and control risk for material financial statement assertions. What could be the areas you look forward for deficiencies and risk identification?	M11 PM	4	Ans - 3
31	You are a member of an audit team of B & C Associates, auditors of a Multinational Company YB Co. Ltd. The company is working in CIS environment. The partner in charge of B & C Associates asked you to draw out the audit plan for evaluating the reliability of controls.	N11 PM	5	Ans - 4

Answer

Ans -1:

Any typical organisation structure would involve different kinds of systems having regard to its nature of operational activities. Apart from the accounting information flow, there may be various other operational departments such as production, sale, purchase, computer department, maintenance, research and development, corporate services, etc. It is quite likely that certain aspects of the organisation have been inter-connected through computers and a central CMS is functional in the organisation. On the other hand, merely because the financial accounting system has not been computerised would not mean that the information generated in other sections of the organisation has no effect on manually maintained accounting records. The auditor's field of interest covers most of the business's activities. For although primarily he will be concerned with the financial accounting department activities, accounting information will be generated by many departments. And it is the auditor's task to see that all this information is reliable. The system of internal control extends beyond those matters which relate directly to the functions of the accounting system. Thus, operational controls such as quality control, budgetary control, quantitative control, work standards, etc. also acquire significance. This is where administrative controls also become important. The auditor should familiarise himself with the tasks being undertaken, the systems that have been developed and the reports generated from such applications. This would provide information which could improve the quality of his own work and enable him to judge better the quality of the accounting systems and internal checks which come within his preview. It would also assist him in making a qualitative judgement as to the state of affairs of the company and give an opportunity to review his audit programme to reduce routine

work and improve quality by assuring that more time is spent by his assistants in other areas to improve quality and offer constructive suggestions. It is very important that the auditor must evaluate such control system also, which have bearing on reliability of financial information.

Ans -2:

A key feature of the accounting software package used by the company definitely involves the absence of clear audit trail. In other words, transactions cannot be easily traced, or co-related from the individual supporting documents.. Moreover, the management does not wish to print the daybooks in view of the voluminous nature since it may involve extensive costs. This has naturally led to extensive dependence by management upon the "exception-reporting" principle.

From the auditor's point to view, it must also be conceded, the exception reports in the form of "query based reports" which isolate the above data provide him with the very material that he requires for most of his verification work. The only problem which it raises and it is a serious one, is that he cannot simply assumes, that the programmes which produce the exception reports are reliable in respect of following facts.

- Operating accurately
- Printing out all the exceptions which exists
- Bound by programmed control parameters which meet the company's genuine internal control requirements?

Therefore in the absence of audit trail, the auditor needs the assurance that the programmes are functioning correctly by using special audit techniques. With special audit technique the auditor starts by proving the accuracy of the input data and then thoroughly examines the processing procedures with the view to establish that:

- All input is actually entered into the computer.
- Neither the computer nor the operators can cause undetected irregularities in the final reports.
- The programmes appear, on the evidence of rejection and exception routines, to be functioning correctly.
- All operator intervention during processing is logged and scrutinized by the EDP manager.

The auditor in such circumstances will have to first evaluate the existing controls. Auditor must do the following:-

- Evaluate the internal control system especially the controls and checks existing for recording the transactions i.e. he has to verify at what level transactions can be entered into the system and what checks are available to prevent any unauthorized data entry and for rectifying errors/omissions in the transactions entered.
- Evaluate at what level there authority is given for modification of transactions already entered. Is there any authority given only to a senior employee to carry out modifications or is it that once transactions are entered and validated no further modification are possible thereto?
- Where there is a provision in the software for carrying out an on line audit of transactions, i.e. Whether there is a separate module in the package, where a separate password given to the auditor and once he has seen and approved a particular transaction/set of transactions, the same would be locked and no modifications would be possible by anyone in the company.
- In case of any loss of data whether there is a clear defined recovery procedure to mini mise the loss of data due to power failures or any human errors.
- The auditor may introduce some dummy data into the system and see the results obtained.

After the auditor has evaluated the above procedures, he has to prepare an audit plan depending on the results obtained from his earlier evaluation. Since the day books are not being printed, the plan can contain procedures wherein data is verified directly on the computer from the voucher, sales invoices etc. the audit plan will also require a lot of analytical procedures to be preformed. Depending on the importance of various expense heads and other important account heads. The auditor will also obtain various reports from the system depending on various queries that he would have to identify.

For example:

- To check whether proper classification is done for revenue/capital - a report can be obtained of all purchases exceeding Rs.2 Lacs. Excluding raw materials or other routine procedures.
- To check whether all freight outward bills are accounted for a report containing a month wise co-relation

between goods dispatched and freight amount paid.

The same can be further co-related with the freight rates obtained from the bills.

Once the auditor has performed the above procedures, he would be able to form an opinion whether reliance can be placed on the accounting systems and the data recorded. If the auditor finds that reliance cannot be placed on the systems, he can inform the management about the fact and also that the day books, etc. will need to be printed to allow him to conduct the audit. The finalization procedures to be followed even under this system would remain more or less similar to other accounting system the auditor can obtain reports of depreciation on fixed assets, inventory valuation and using the normal procedures find out whether reliance can be placed on them. Similarly, depreciation calculations will have to be verified on a random basis to find out its reliability.

Ans -3:

The auditor in accordance with SA 315 "Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and its Environment", should make an assessment of inherent and control risk for material financial statement assertions.

In a CIS environment the risk of a Material financial statement could arise from the deficiencies in the following case as

- Program Development and maintenance.
- System Software supports.
- Operations including processing of data
- Physical CIS security.
- Control over access to specialized utility program.

These deficiencies would tend to have a negative impact on all application systems that are processed through the computer.

Ans -4: Audit Plan for Evaluating the Reliability of Controls in CIS Environment:

In evaluating the reliability of controls in CIS environment, the auditor needs to assess the reliability by considering the various attributes of a control. Some of the attributes for example are that, the control is in place and is functioning as desired. General V/s specific control with respect to the various types of errors and irregularities that might occur, general control inhibit the effect of a wide variety of errors and irregularities as they are more robust to change controls in the application sub-system which tend to be specific control because component in these sub-system execute activities having less variety, that whether the control acts to prevent, detect or correct errors etc. The auditor focuses here on

- **Preventive Controls:** They stop errors or irregularities from occurring.
- **Detective Controls:** They identify errors and irregularities after they occur.
- **Corrective Controls:** They remove the effects of errors and irregularities after they have been identified.

The auditors are expected to see a higher density of preventive controls at the early stages of processing or conversely they expect to see more detective and corrective controls later in system processing.

Further while evaluating the reliability of controls, the auditor should refer Point No. 14 of this Chapter.

A COMPLETE GUIDE FOR
ADVANCED AUDITING

(CA FINAL)

Salient Features

- Presentation of whole Syllabus in an easy language to understand the complex subject matter.
- Tabular and graphic presentation to facilitate easy understanding and learning.
- Inclusion of flowcharts on various topics, including Standards on Auditing.
- Presentation of maximum topics in point-wise manner.
- Upto date Amendments Including CARO 2015 & Format of New Audit Report Under Companies Act, 2013.
- Illustration of all "Audit Report" as per SA 700, SA 705 & SA 706 at one place (See Chapter 24) for quick understanding of "Audit Report" in different situations with minimum time frame & fast understandability.
- All Example of Engagement Letter as per SA 210, SA 2400, SRE 2410, SRS 4400, SRS 4410 at one place (See Chapter - 24) for quick understanding of Engagement Letter in different situations with minimum time frame & fast understandability.
- All Illustration of Audit Report, Review Report & Certificate as per SA 800, SA 805, SRE 810, SRE 2400, SRE 2410, SAE 3400, SRS 4400, SRS 4410 at one place (See: Chapter - 24) for quick understanding of Audit Report, Review Report in different situations & their comparison with minimum time frame & fast understandability.
- Full coverage of Questions appeared in past 35 exams & Practice Manual has been arranged in following manners:
  - « Chapter wise/topic wise
  - « Standard of Auditing wise
  - « Accounting Standard wise
  - « Clause wise & Schedule wise (Chapter – Professional Ethics)
  - « Clause wise (Chapter – Audit under Fiscal Law (Form 3CD)
- Graphs at the beginning of every chapter, showing marks allotment in last twenty examinations.
- List of questions including case study's appeared in past 34 examinations given at the end of each chapter. Suggested answer given after Questions, so that student could first try to recall the Law/ points/SA/Section/Act related to that case study and try to solved out the case study before seeing the suggested answer. It will enhance their irretrievability power. It will also help students to have an idea of paper style.
- Short Notes of all Chapters given at the end of the book (See Chapter – 26) for Quick revision.
- Table Showing Importance of Chapter on the Basis of Marks Allotment in Past Examinations.
- 100 + practical Question on New Companies Act, 2013 & CARO 2015.

Available at Leading Bookshops all over India, or write to:
Spiraa™ Publishing Inc.
Phone: 011-45553634 Email: info.spiraa@gmail.com
Also Available on amazon.in and flipkart.com

ISBN 819305801-1
9 788193 058015