1. WHAT IS AN AUDIT TRAIL?

❖ **Meaning:**

   a) Audit Trail can be defined as the 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.

   b) Audit Trail is the visible means by which the auditor may trace a business transaction through all the stages in which it features in the records of the business.

     (Recruitment records from HR → Attendance records from gate office → Overtime records from factory → tax saving records from finance → Wage computation register → Wage slip → payment receipt → Cash book → monthly journal entry → Wages A/c → Employee benefit cost in p&l)

❖ **Purpose:**

Audit Trail is need to –

   a) Fulfill statutory requirements, *(obtain all evidence)*

   b) Answer queries, *(Obtain understanding & tell it to seniors)*

   c) Minimize irregularities, *(frauds & errors detection)*

   d) Detect the consequence of error, etc. *(effects on financial statements)*

❖ **Examples:**

Sequentially numbered Sales Invoice copies would normally be listed in a Register or Daybook and subsequently filed either in numerical or chronological sequence. It would be possible, to trace a particular invoice from the daybook to the original on file or vice-versa, by reference to the number or the date of the invoice. *(Small example of audit trail sales invoice to sales register using invoice numbers)*

❖ **Types:**

   a) The **Accounting Trail** shows the source and nature of data and process that update the database. *(above given example is of accounting trail)*

   b) The **Operations Audit Trail** maintains records of attempted or actual resource consumption within a system. *(number of hour spent by labours on each floor, each site or type of work)*

      *(quantitative consumption of raw material, number of hours of labours, machine hours spent on product manufacturing)*

❖ **Effect on Audit:**

In a manual system, it is possible to related the recording of transaction at each successive stage enabling an Auditor to locate and identify all documents from beginning to end for the purpose of examining documents, totaling and cross – referencing. Such comparison may not be possible in a CIS environment.

❖ **How to compensate Audit Trail**

   1) Auditor can ask the client to arrange for **special print-outs** of additional information. *(Of all documents as discussed above)*

   2) **Tagging and Tracing**

      I. It is used for compensating loss of audit trail.

      II. It involves tagging the clients input data in such a way that relevant information is displayed at key points to be verified by the auditor. *(High Salary Employees, Overtime*
more than 50%, Leaves more than 10 in a month, bonus more than 2-month salary etc)

III. The hard copy generated is made available only to the auditor. For e.g. sales order in excess of 2.5 lakhs etc.

IV. It uses actual data, thus question of elimination of special entries (as in integrated test data facility) does not arise at all.

However, all erroneous data may not necessarily be tagged.

Auditor uses his professional judgment to decide the key point.

3) Clerical recreation. (manually generation of figures which have been created by computers)

4) Testing on total basis. (If individual items can’t be checked in detail, then auditor may resort to testing on total basis).

5) Relying on alternative tests. (i.e., checking other documents etc. like in manual system)

6) Special Audit Technique. (CAAT)

2. IMPACT OF COMPUTERISATION (On Audit Approach)

Impact of computerisation on audit approach needs consideration of the following factors:

HDR- SMILE

(1) High speed - In a CIS environment information can be generated very quickly. Even complex reports in specific report format can be generated for audit purposes without much loss of time. This cut down the time enabling the auditor to extend their analytical review for under coverage with high speed of operation, the Auditor can expand their substantive procedures for collection of more evidence in support of their judgement.

(With manual records on monthly wage analysis was possible, but now we can do it site wise, skill wise, age wise, construction cost per square feet etc.)

(2) Disappearance of manual Reasonableness - The shift from traditional manual information processing environment to computerised information systems 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. (Auditor may select few items for sale sampling on basis of judgement for Eg new sales executive, dominant executive, one who has heavy expenditure, peak time etc and then apply random sampling etc but now in automated sampling these options may not be possible so this manual reasonableness may not be possible.)

(3) 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 thereby concentrating the duties of several personnel involved in the work. (Eg Earlier separate individuals were sent for each salary for each location but now only person sitting on centralised system will be able to do it.)

(4) Shifting of internal control base –
(Earlier knowledge, personal ethics and character were most important factors but now it changed to following.)

(i) Application systems development control - Systems development control should be designed to provide reasonable assurance that they are developed in an authorised and efficient manner, to establish control, over: (Inventory / Employee / Production / Billing module, NPA module etc)

(a) testing, conversion, implementation, and documentation of new revised system.

(b) changes to application system.

(c) access to system documentation.
(d) acquisition of application system from third parties.

(ii) Systems software control - Systems software controls are designed to provide reasonable assurance that system software is acquired or developed in an authorised and efficient manner including: (DOS, Windows, Linux, OS, Android, Chrome Book etc)

(a) authorization, approval testing, implementation and documentation of new system software systems software modifications.

(b) putting restriction of access to system software and documentation to authorised personnel.

(5) Man-machine interface / human-computer interaction - Man-machine interface ensures maximum effectiveness of the information system. Organization concentrated on presenting information that is required by the user and to present that information in the most uncluttered way. It is required to determine what information was necessary to achieve through a careful analysis of the job or task for which the user needed the information.

Human-computer interaction is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of the major phenomena, surrounding them. The approach is user centered and integrates knowledge from a wide range of disciplines. (Writing programming codes→ Writing Commands→ Then using Clicks→Then using TOUCH→Now Voice Recognition→Then brain Signals→ Then intuitions.)

(6) Impact of poor system - If system analysis and designs falls short of expected standard of performance, a computerised information system environment may do more harm to integrated business operation than good. Thus, care has to be taken in adopting manual operations switchover to computerised operations for ensuring performance quality standards. (not able to absorb client data, tedious manual process of editing data before processing, such things complicates a nd decreases speed of auditing.)

(7) Low clerical error - Computerised operation being a systematic and sequential programmed course of action the changes of commission of error is considerably reduced. Clerical error is highly minimised. (Eg debit credit generally tallies, totalling errors are eliminated, so focus of auditor shifts to error of principle, compensating errors etc.)

(8) Exception reporting - This is a part of Management information system. Exception Reporting is a departure from straight reporting of all variables. Here the value of a variable is only reported if it lies outside some pre-determined normal range. This form of reporting and analysis is familiar to the accountant. The main strength of exception reporting lies in its recognition that to be effective information must be selectively provided. (Eg Increase in expense of particular account is more than 50%, negative inventory, negative cash or bank etc these can be used by auditor)

3. IMPACT OF CHANGES ON BUSINESS PROCESSES (FOR SHIFTING FROM MANUAL TO ELECTRONIC MEDIUM)

The effect of changes on accounting process may be stated as under:

A. Primary Changes: -

(1) Process of recording transactions - The process of recording transaction undergoes a major change when accounting process are computerised under CIS environment, the order of recording transaction from basic document to prime books and finally to principal book may not be followed strictly in sequential form as is observed in manual system. In many cases all the three processes Prime book of Entry, Ledger, Final accounts (Balance Sheet and Profit and Loss Account) are carried on simultaneously. (Daily Voucher → Weekly Journal → Monthly Ledger→Quarterly Trial Balance & Financial Statement. Now simultaneous voucher / journal / trial balance / financial statement)

(2) Form of accounting records - Mechanisation often results in the abandonment in whole or in part of the primary records. Punch card installation or electronic data processor changes the form of both
intermediate and ultimate records much more radically than manual records. *(Signature based attendance register to punch card system, so register is eliminated and now accurate in and out time are recorded, earlier employees use to submit Over Time claim but now it is system generated, instead of printed salary slip, email of pdf so final record has also changed, earlier computations and other details were not printed but now included in pdf as it doesn’t affect cost.)*

(3) **Use of loose-leaf stationeries** - Bound hand-written records as used in manual accounting processes are replaced by loose-leaf machine written records in electronic medium. In a computerised information system, magnetic tapes, floppy disks, diskettes, print-outs replace the traditional records. This necessarily require proper control over such records to prevent their unauthorised use, destruction or substitution. *(Earlier pre-numbered red colour registers were used, where changes are visible and pages cannot be torn, on the other hand electronic records can be changed without any trace.)*

(4) **Use of accounting code** – In computerised information systems, alpha-numeric codes are extensively used to represent names and description. The accountants as well as the Auditors have to get themselves familiarised with the use of such codes which initially may pose considerable problems in understanding the various transactions. *(First select account code then product code then profits centre number then employee code to record sales.)*

(5) **Absence of link between transaction** – In a computerised information system environment, there may be an inadequacy or even total absence of cross-reference between the basic documents, primary records and the principal records. This creates special problems for the auditors. The auditors may find it difficult to trace a transaction from start to finish there by having a doubt in their mind as to loss of audit trials. *(Take example of Question 1)*

B. Recent Changes
The growth and development in the field of information technology is a fast paced one and unless the auditors are alert to such developments and take pre-emptive action in upgrading their knowledge, they may find difficulty in coping with such advancement.

Following are a few instances of the recent changes which may need to be addressed in discharging their responsibilities in such environment:

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

4. **AUDIT APPROACHES IN A CIS ENVIRONMENT**

Based on the knowledge and expertise of Auditors in handling computerized data, the audit approach in a CIS environment could be either:

A. The Black-box approach i.e., Auditing around the computer, or
B. The White-box approach i.e., Auditing through the computer.
A. The Black Box Approach
In the Black box approach or Auditing around the computer, 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.

In testing, say, Payroll Application, the auditor might first examine selected time cards for hours worked and employee earning cards for rates and then trace these to the payroll summary output and finally compare hours, rates and extensions. The comparison of inputs and outputs may be done manually with the assistance of the computer. The computer assisted approach has the advantage of permitting the auditor to make more comparisons than would be possible, if done manually.

Auditing around the computer has the advantage of ease of comprehension as the tracing of documents to output does not require any in-depth study of application program.

A major disadvantage, however, is that the auditor not having directly tested the control, cannot make assertions about the underlying process. Moreover, in some of the more complex computer systems intermediate printout may not be available for making the needed comparisons.

B. The White Box Approach
The processes and controls surrounding the subject are not only subject to audit but also the processing controls operating over this process are investigated. In order to help the auditor to gain access to these processes computer Audit software may be used. These packages may typically contain: **(Similar to uses of CAAT as in this approach we use CAAT)**

(a) interactive enquiry facilities to interrogate files.
(b) facilities to analyze computer security logs for unusual usage of the computer.
(c) the ability to compare source and object (compiled) program codes in order to detect dissimilarities.
(d) the facility to execute and observe the computer treatment of "live transaction" by moving through the processing as it occurs.
(e) the generation of test data.
(f) the generation of aids showing the logs of application programs. The actual controls and the higher-level control will be evaluated and then subjected to compliance testing and, if necessary, substantive testing before an audit report is produced.

It is obvious, that to follow this approach the auditor needs to have sufficient knowledge of computers to plan, direct-supervise and review the work performed.

The areas covered in an audit will concentrate on the following controls:
(1) Input controls,
(2) Processing control,
(3) Storage control,
(4) Output control and
(5) Data transmission control.

The auditor will also need to be satisfied that there are adequate controls over the prevention of unauthorized access to the computer and the computerized database. The auditors task will also involve consideration of the separation of functions between staff involves in transaction processing and the computerized system and ensuring that adequate supervision of personnel is administered.

The process of auditing is not a straightforward flow of work from start to finish to be completed by satisfying oneself against a standard checklist or a list of questions. It involves exposure, experiences and application of knowledge and expertise to differing circumstances.

**No two-information system is same.** From the view point of analysis of computerized information system, the auditors need not only have adequacy on knowledge regarding information requirement and computer data security they must also get exposed to system analysis and design so as to facilitate post implementation audit.
**5. EFFECT OF COMPUTERS ON INTERNAL CONTROLS**

Internal control system includes separation of duties, delegation of authority and responsibility, a system of authorization, adequate documents and records, physical control over assets and records, management supervision, independent checks on performance and periodic reconciliation of assets with records. In CIS environment, all these components must exist but computers affect the implementation of these internal controls in many ways. Some of the effects are as under:

**S&P are ADDICTS of Internal Controls**

(1) Segregation of Duties - In a manual system, different persons are responsible for carrying out function like initiating, recording of transaction, safeguarding of assets, does not always apply in a computer system. For example, in a computer system, a program may carryout reconciliation of vendor invoice against a receipt document and also prepares a cheque payable to trade payables. Such operation through a program will be considered as incompatible functions in a manual system.

In minicomputer and microcomputer environments, separation of incompatible function could be even more difficult. Some such forms, allows, users to change programs and data entry without providing a record of these changes. Thus, it becomes difficult to determine whether incompatible function have been performed by system users. *(Purchase Accountant is given authority to change forms etc in system to keep it updated and easy to use.)*

(2) 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 are shared among multiple users. For instance, one objective of using a data base management system is to provide multiple users with access to the same data, thereby reducing the control problems that arise with maintaining redundant data, when multiple users have access to the same data and the integrity of the data is somehow violated, it is not always easy to trace who is responsible for corrupting the data and...
who is responsible for identifying and correcting the error. Some organization identified a single user as the owner of the data.

(3) **Competent and Trustworthy Personnel** - Skilled, competent, well-trained and experienced information system personnel have been in short supply. Since substantial power is often vested in the person responsible for the computer information system development, implementation, operation and maintenance within the organization, competent and trustworthy personnel is very much in demand. Unfortunately, the non-availability of competent personnel, forced many organization to compromise on their choice of staff. Moreover, it is not always easy for Organization to assess the competence and integrity of their system staff. High turnover among those staff has been the norm. Some information systems personnel lack a well-developed sense of ethics and some enjoy in subverting controls.

(4) **System of Authorization** - Management authorization of transaction may be either:
(a) general authorization to establish policies for the Organization, *(for routine matters, such as credit sales approval)*
(b) specific authorization applying to individual transactions. *(for non-routine matters, such as property acquisition)*

In manual system, auditors evaluate the adequacy of procedures for authorization by examining the work of employees *(Examining approvals made by them)*.

In a computer system, authorization procedures often are embedded within a computer program. In a computer system, it is also more difficult to assess whether the authority assigned to individual persons is constant with managements policies. Thus, in evaluating the adequacy of authorization procedures, auditors have to examine not only the work of employees but also the veracity of the programme processing. *(Examining software settings & approvals made by them)*.

(5) **Adequate Documents and Records** - In a manual system, adequate documents and records are required to provide an audit trail of activities within the system. In computer system, document support might not be necessary to initiate, execute and records some transaction. The task of a visible audit trail is not a problem for auditors, provided the systems have been designed to maintain a record of all events and that they are easily accessible. In well-designed computer systems, audit trails are more extensive than those maintained in manual systems unfortunately not all computer systems are well designed. This creates a serious control problem.

(6) **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 concentration of information systems assets and record also increases the losses that can arise from computer abuse or disaster. If the Organization does not have another suitable backup, it might be unable to continue operations.
(7) **Adequate Management Supervision** - In a computer system, supervision of employee might have to be carried out remotely. Supervisory controls must be built into the computer system to compensate for the controls that usually can be exercised through observation and inquiring computer system also make the activities of employees less visible to management. Because many activities are electronically controlled managers must periodically access the audit trial of employee activities and examine it for unauthorized actions.

(8) **Independent Checks on Performance** - Checks by an independent person help to detect any errors or irregularities. In a computer system, if a program code is authorized accurate, and complete the system will always follow the laid down procedures in absence of other type of failures like hardware or systems software failure. Thus, independent checks on the performance of programs often have little value. Instead, the control emphasis shifts to ensuring the veracity of programme code. Auditors must now evaluate the controls established for program development, modification operation and maintenance.

(9) **Comparing Recorded Accountability with Assets** - In a manual system, independent staff prepares the basic data used for comparison purposes. In a computer system software is used to prepare this data. If unauthorized modifications occur to the program or the data files that the program uses, an irregularity might not be discovered, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.

---

### 6. EFFECTS OF COMPUTERS ON AUDITING

The objective of auditing, do not undergo a sea change in a CIS environment. Auditor must provide a competent, independent opinion as to whether the financial statements records and report a true and fair view of the state of affairs of an entity. However, computer systems have affected how auditors need to collect and evaluate evidence. These aspects are discussed below:

(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, like:

   (a) accurate and complete operations of a disk drive may require a set of **hardware controls** not required in manual system,

   (b) **system development control** includes procedures for testing programs that again are not necessary in manual control.

Since, Hardware and Software develop quite rapidly, understanding the control technology is not easy. With increasing use of data communication for data transfer, research is focused on cryptographic controls to protect the privacy of data. **Unless auditor’s keep up with these developments, it will become difficult to evaluate the reliability of communication network competently.**

The continuing and rapid development of control technology also makes it more difficult for auditors to collect evidence on the reliability of controls. Even collection of audit evidence through manual means is not possible. Hence, auditors have to run through computer system themselves if they are to collect the necessary evidence. Though generalized audit software’s are available the development of these tools cannot be relied upon due to lack of information. Often auditors are forced to compromise in some way when performing the evidence collection.

(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. Auditors need to understand:
(a) whether a control is functioning reliably or multi functioning,
(b) traceability of control strength and weakness through the system. In a shared data environment, a single input transaction may update multiple data item used by diverse, physically disparate user, which may be difficult to understand. Consequences of errors in a computer system are a serious matter as errors in computer system tend to be deterministic, i.e., an erroneous program will always execute data incorrectly. Moreover, the errors are generated at high speed and the cost and effort to correct and rerun program may be high. Errors in computer program can involve extensive redesign and reprogramming. Thus, internal controls that ensure high quality computer systems should be designed implemented and operated upon. The auditors must ensure that these controls are sufficient to maintain assets safeguarding, data integrity, system effectiveness and system efficiency and that they are in position and functioning.

7. INTERNAL CONTROLS IN A CIS ENVIRONMENT

SPE³A⁴R system has all controls

(1) Authenticity Controls - Authenticity control is exercised to verify the identity of the individuals or process involved in a system (e.g. password control, personal identification numbers, digital signatures). *(Security Question, Name of your PET?)*

(2) Accuracy Control - Accuracy control ensure the correctness of data and processes in a system (e.g. program validation check that a numeric field contains only numeric, overflow checks, control totals, hash total etc.). *(ICAI Exam form, Student Registration Number Check)*

(3) Completeness Control - Completeness control attempt to ensure that no data is missing and that all processing is carried through to its proper conclusion (e.g. program validation check, sequence check etc.).

(4) Redundancy Control - Redundancy controls attempt to ensure that a data is processed only once (e.g. batch cancellation stamp, circulating error files etc.).

(5) Privacy Controls - Privacy controls ensure that data is protected from inadvertent or unauthorised disclosure (e.g. cryptograph, data compaction *(FYI For Your Information)*, inference control etc.). *(In table a1, a2, a3, a4 may be represented by Male_Married, Male_Unmarried, Female_Married and Female_Unmarried)*

(6) Audit Trail Controls - Audit trail control ensures traceability of all events occurred in a system. This record is needed to answer queries, fulfil statutory requirements, minimise irregularities, detect the consequences of error etc. The accounting audit trail shows the source and nature of data and process that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

(7) Existence Controls - Existence controls attempt to ensure the ongoing avail ability of all system resources (e.g., database dump and logs for recovery purposes duplicate hardware, preventive maintenance, check point and restart control).

(8) Assets Safeguarding Controls - Asset safeguarding control attempt to ensure that all resources within a system are protected from destruction or corruption (e.g. physical barriers, libraries etc.).

(9) Effectiveness Controls - Effectiveness control attempt to ensure that systems achieve their goals (e.g. monitoring of user satisfaction, post audits, periodic cost benefit analysis etc.)

(10) Efficiency Controls - Efficiency controls attempt to ensure that a system uses minimum resources to achieve its goals. *(standard labour cost per unit vs actual labour cost.)*
The following points describe the General Audit Approach in a CIS Environment:

1. Skills and Competence:
   a) The auditor should have sufficient knowledge of the CIS Environment, to plan, direct, supervise, control and review the work performed. *(Need Sap Training)*
   b) The Auditor should consider whether any specialized CIS skills are needed in the conduct of the audit, and if yes, the auditor should seek the assistance of an Expert possessing such skills. *(Need SAP Expert)*

2. Planning:
   a) The Auditor should obtain an understanding of the significance and complexity of the CIS activities, and the availability of the data for use in the audit.
   b) The Auditor should also obtain an understanding of the accounting and internal control system, to plan the audit and to determine the nature, timing and the extent of the audit procedure.
   c) Auditors understanding of CIS process would include:
      - CIS Infrastructure (hardware, operating system(s) and application software used by the entity, including changes therein since last audit, if any) *(Intel Vs AMD / Windows Vs IOS)*
      - Significance and complexity of computerized processing in each significant accounting application, (Significance relates to materiality of the financial statement assertions affected by the computerized processing.) *(Sales commission is significant and dependent on system, Eg Achieving sales with low bad debts)*
      - Organizational structure of the Client, CIS activities and the extent of concentration or distribution of computer processing throughout the entity, particularly as they may affect segregation of duties. *(HOD is having all powers, his knowledge and character is very important)*
      - Extent of availability of data by reference to source documents, computer files and other evidential matters. CIS may generate reports that might be useful in performing substantive tests (Particularly analytical procedure). The potential for use of CAATs may permit increased efficiency in the performance of audit procedures, or may enable the Auditor to economically apply certain procedures to the entire population of transactions. *(Monthly charts of accounts for analytical procedures)*

3. Risk Factors Analysis: The Auditor should assess whether CIS may influence the assessment of inherent and control risks. The nature of risks in CIS Environment include the Following – DISCUS-IT
   a) Lack of Transaction Trails: - Some computer information system are designed so that a complete transaction trail that is useful for audit purpose might exist for only a short period of time or only in computer readable form. Where a complex application system performs a large number of processing steps, there may not be a complete trail. Accordingly, errors embedded in an application’s program logic may be difficult to detect on a timely basis by manual procedures. *(Missing monthly salary computation)*
   b) Uniform Processing of transactions: - Computer programs process transaction uniformly, virtually eliminating the occurrence of clerical errors. But, if programming error exists, all transaction will be processed incorrectly. *(Salary for the day Sal / 26 , if system uses 30 all calculations will go wrong)*
   c) Lack of Segregation of functions: - Many controls become concentrated in a CIS Environment, allowing for combination of incompatible functions. *(Purchase / Receipt & Payment of goods is through same software)*
   d) Potential for Errors and Irregularities: The potential for human error in the development, maintenance and execution of CIS may be greater than in manual system, because of the level of detail inherent in these activities. Also, the potential for individuals to gain unauthorized access to data or to alter data without visible evidence may be greater in CIS environment than in manual systems. *(New types such as unauthorized changes in data from remote location)*
e) **Initiation or Execution of Transactions:** In a CIS process, certain types of transaction are triggered internally by the system, the authorization for which may not be documented as in manual system. In such cases, Management's authorization of these transactions may be implicit/implied. *(System generated interest calculations)*

f) **Need of CAAT:** The Auditor may apply general or specialized computer audit techniques and tools in the execution of audit tests. There is a risk that certain errors may not be detected by CAAT, in case of sample testing process. *(CAAT may fail because of sampling error or risk)*

g) **Dependence of Other Controls over Computer Processing:** Certain manual control procedures are dependent on computer generated reports and outputs for their effectiveness. In turn, the effectiveness and consistency of transaction processing controls are dependent on the effectiveness of general CIS controls. *(Exception reporting and then manual scrutiny)*

h) **Increased Management Supervision:** CIS can offer Management a variety of analytical tools, which can enhance the effectiveness of the entire internal control structure. *(Real time sales data and weekly costing data and monthly profitability)*

4. Evaluating reliability of controls: While evaluating the reliability of the accounting and internal control systems, the Auditor would consider whether these systems –
   a) Ensure that **authorized, correct and complete data** is made available for processing.
   b) Provide for **timely detection and correction of errors**.
   c) Ensure that the case of **interruption in the work of the CIS environment due to power, mechanical or processing failures,** the system re–start without distorting the completion of the entries and records.
   d) Ensure the **accuracy and completeness of output**.
   e) Provide **adequate data security against fire and other calamities, wrong processing, frauds, etc.**
   f) Prevent unauthorized amendments to programs. Provide for safe custody of source code of application software and data files.

5. Documentation: The auditor should document the audit plan, the nature, timing and extent of audit procedure performed and the conclusions drawn from the evidence obtained.

   a) In an audit in CIS environment, some of the audit evidence may be in electronic form. The Auditor should satisfy himself that such evidence is adequately and safely stored and is retrievable in its entirety as and when required.

### 9. GENERAL EDP CONTROLS VS APPLICATION EDP CONTROLS

Describe the major types of Internal Controls in a CIS Environment based on areas/aspects covered.

Internal Controls under CIS Environment cover the following aspects/areas –

<table>
<thead>
<tr>
<th>Control</th>
<th>Aspects covered / Objectives of Control</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GENERAL EDP CONTROLS</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **1. Organization & Management Control** | To establish an organizational Framework for CIS activities including-
- Policies and procedures relating to control functions, and
- Appropriate segregation of incompatible functions. *(programmer & checker should be different)* |
| **2. Computer Operation Controls** | To Control the operation of the system, and provide reasonable assurance that-
- Systems are used for authorized purposes only. *(no personal use)*
- Access to computer operation is restricted to authorized personnel, *(Computers are fixed per person)*
- Only authorized programs are to be used, and *(No share trading software)*
- Processing errors are detected and corrected. *(Everyone takes its own*
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 3. **System Software Control** | To provide reasonable assurance that system software is acquired or developed in an authorized and efficient manner including-  
• Authorization, approval, testing, implementation and documentation of new system software and system software modification.  
• Restriction of access to system software and documentation to authorized personal.  
*Note at the start that this installation is verified, and settings can be changed only by admin* |   |
| 4. **Data Entry and Program Control** | To provide assurance that-  
• An authorization structure is established over transaction being entered into the system, and  
• Access to data and program is restricted to authorized personnel. |   |
| 5. **Application System Development & Maintenance Control** | To provide reasonable assurance that systems are developed and maintained in an authorized and efficient manner, to establish control over –  
• Testing, conversion, implementation and documentation of new revised system,  
• Changes made to application system  
Access to system documentation, and  
Acquisition of application system from third parties. |   |
| 6. **Continuity Controls** | To contribute to the continuity of CIS Processing, and include-  
• Offsite back-up of data and program,  
• Recovery Procedure for use in the event of theft, loss or intentional or accidental destruction, and  
• Provision of off-site processing in the event of disaster. |   |
| **Application EDP Controls** | To provide reasonable assurance that –  
• Transaction are properly authorized before being processed by the Computer,  
• Transaction are accurately converted into machine-readable form and recorded in the computer data files,  
• Transaction are not lost, added, duplicated or improperly changed, and  
• Incorrect transaction are rejected, corrected and if necessary, re-submitted on a timely basis. |   |
| 7. **Control Over Input** | To provide reasonable assurance that –  
• All transaction including system generated transaction are properly processed by the computer,  
• Transaction are not lost, added duplicated or improperly changed,  
• Processing errors are identified and corrected on a timely basis. |   |
| 8. **Control Over Processing and Computer Data Files** | To provide reasonable assurance that –  
• Result of processing are accurate,  
• Access to output is restricted to authorized personnel, and  
• Output is provided to appropriate authorized personnel on a timely basis. |   |
| 9. **Control Over Output** |   |   |
10. ORGANIZATION STRUCTURE AS CONTROLS ASPECT

"Organization Structure", as a Control Aspect in CIS Environment

CIS function in an entity should be properly organized, such that different groups are formed to perform different some of the typical functions that must be performed are-

<table>
<thead>
<tr>
<th>Position/ Function</th>
<th>Duties and Responsibilities</th>
</tr>
</thead>
</table>
| 1. Data Administrator | a) Generates the data requirements of the users of information system services,  
b) Formulates data policies, plans the evaluation of the corporate data bases, and  
c) Maintains data documentation |
| 2. Database Administrator | (a) Responsible for the operational efficiency of Corporate Database, and  
(b) Assists Users to use database better. |
| 3. System Analyst | a) Manages information requirements for new and existing applications,  
b) Designs information systems architectures to meet these requirements,  
c) Facilitates implementation of information systems,  
d) Writes procedures and users documentation |
| 4. System Programmer | a) Maintains and enhances operating system software, library software, network software, library software and utility software.  
b) Provide support when unusual systems failure occurs. |
| 5. Application programmer | a) Deigns programs to meet information requirement,  
b) Codes, tests and debugs programs,  
c) Documents programs, and  
d) Modify programs to remove errors and improve efficiency. |
| 6. Operation specialist | a) Plans and controls day to day operations,  
b) Monitors and improve efficiency along with capacity planning. |
| 7. Librarian | a) Maintains library of magnetic media and documentation  
b) Acts as Custodian of Master Files & Programs,  
c) Permits access to systems and data files as per authority, and  
d) Safeguards against unauthorized access. |

Auditors Duties: -  
a) Responsibilities of each job position must be clear, and incumbents (Outgoing Person) must fully understand their duties, authority and responsibilities.  
b) Jobs performed within the information system function should maintain the principle of separation of duties to the extent possible. Without separation of duties, errors and irregularities might remain undetected.

11. ACCESS CONTROL IN CIS ENVIRONMENT

Access Controls may seek to - (a) prevent persons who are authorised for access, from accessing restricted data and programs, and (b) prevent unauthorized persons from gaining access to the system as a whole. Access Controls may take any of the following forms –
## Types of control and Purpose of control

<table>
<thead>
<tr>
<th>Types of control</th>
<th>Purpose of control</th>
</tr>
</thead>
</table>
| **1. Limited physical**  
**(to the computer facility)** |  
| a) Physical Facilities that hold the computer equipment, files and documentation, should have controls to limit access only to authorized individuals.  
b) Types of controls include –  
1. Security Personnel,  
2. Automated key cards,  
3. Manual key locks,  
4. Access device like fingerprint, palm prints, or other biometric device. |
| **2. Hardware & software access control** |  
| a) Access control software like user identification may be used. This is a frequently used control, and is a combination of unique identification code and confidential password. |
| **3. Call back** |  
| a) It is a specialized form of user identification in which the User dials the system, identifies himself and is disconnected from the system. Then, either an individual manually finds the authorized telephone number or the system automatically finds the authorised telephone number of individual, and the user is called back. Then, the User is permitted access to the system.  
**{(Income Tax / Bank Transactions)}** |
| **4. Visitor entry logs** |  
| a) Entry logs should be used to determine and document who have had access to the area. |
| **5. Encryption** |  
| a) In encryption, data is encoded when stored in computer files, and/ or before transmission to or from remote locations.  
b) This coding protect data because, to use the data unauthorized users must not only obtain access, but must also decrypt the data, i.e. decode it from encoded form. |
| **6. Segregation Controls** |  
| a) Access to Program Documentation should be limited to those persons who require it in the performance of their duties.  
b) Access to Data Files and Programs should be limited to those individuals authorized to process data.  
c) Access to Computer Hardware should be limited to authorized individuals  
(e.g. Computer Operators/ specified Users). |
| **7. Computer Application Controls** |  
| a) Programmed applications Application Controls apply to specific applications rather than multiple applications.  
**{(Username Password of specific software, for example pin to open paytm)}** |

---

### 12. EXPLAIN THE CONCEPT OF INPUT CONTROL IN A CIS ENVIRONMENT

Input into the CIS system should be properly authorized and approved. The system should verify all significant data fields used to record information, i.e. it should perform editing of the data. Conversion of data into machine readable form should be controlled and verified for accuracy. For validation of input, the following controls are generally applied-

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Pre – printed Forms</strong></td>
<td></td>
</tr>
</tbody>
</table>
| (a) Standard information and instruction for filling should be printed on a source document.  
(b) For example, if only limited number of responses to a question is considered appropriate, then pre-print the responses, e.g. Yes, No, not Applicable, and have the user tick or circle the correct responses deleting those that are inappropriate. |
2. Check Digit

(a) Errors made in transcribing and keying data can be reduced by using ‘Check Digit’ Control.
(b) A Check Digit is a redundant digit added to a code that enables the accuracy of other characters in the code to be checked.
(c) The check Digit can act as a prefix or suffix character, or it can be placed somewhere in the middle of the code.
(d) When the codes are entered, a program re-calculates the check digit to determine whether the entered check digit and the calculated check digit are the same. If they are the same, the code is most likely to be correct.

3. Completeness Total

The purpose of this control is to ensure that no data is left out completely form being entered into the system, some Example are –

(a) **Sequence Checks**: Documents may be pre-numbered sequentially before entry, and at a later stage the computer will perform a sequence check and display any missing number.

(b) **Batch Record Totals**: The number of transaction is counted manually, and this is compared with the record count produced by the computer at the end of the batch.

(c) **Batch Control Totals**:
   - The transactions are collected together in batches of say, 50 transactions.
   - A total of all the data value of some important field is calculated manually, e.g. Total Sales Value for a batch of 50 invoices.
   - The control total is then compared with a computer-generated control total, after input of batch transaction. A difference indicates either a lost transaction or the input of an incorrect invoice total.
   - This method is not fool proof, since compensating errors are possible.

(d) **Batch Hash Total**: the idea is similar to control totals, except that Hash Totals prepared purely for control purposes. The total of all Invoices Numbers in a batch is meaningless, but may be used for control by comparing it with computer-generated hash totals.

4. Reasonableness Check

These are sophisticated forms of limit Checks. An example might be a check on an electricity meter reading. The check might consist of subtracting the last reading recorded from the current reading and comparing this with the average usage for that period. If the reading differs by a given percentage, then it is investigated before processing.

5. Field Checks

The following types of field checks may be applied –

(a) **Missing Data / Blank**: is there any missing data in the field? If a code should contain 2 hyphens, though they might be in a variable position, can only one be detected? Do the filed contain blanks when data always should be present?

(b) **Alphabetic / Numeric**: Does a field that should contain only alphabetic or numeric contain alphanumeric characters?

(c) **Range**: Does the data for a field fall within its allowable value range? **(Product codes are between 100 to 999)**

(d) **Master Reference**: if the Master file can be referenced at the same time input data is read, is there a Master file match for the key Field.

(e) **Size**: If variable length fields are used and a set of permissible sizes is defined, does the field delimiter show the field to be one of these valid sizes?

(f) **Format**: Data entered into a field might have to conform to a particular format like ‘dd/mm/yyyy’
6. Record Checks

The following types of Records Checks can be applied –

(a) Reasonableness: Even though a field value might pass a range check, the content of another field might determine what a reasonable value for the field is. (For example, salary field will be not be more than 1,00,000 if post is below senior manager)

(b) Valid – sign – Numeric: The content of one field might determine which sign is valid for a numeric field. (If money field shows received in cash transaction then amount field should be positive)

(c) Size: if variable length records are used, the size of the record is a function of the sizes of the variable length fields or the sizes of fields that optionally might be omitted from the record. The permissible size of the fixed and variable length records also might depend on a field indicating the record type.

7. File Checks: In file Checks, validation control examines whether the characteristics of a file used during data entry are matching with the stated characteristics of the file. For example, if Auditors validate some of the characteristic of data that is keyed into an application system against a Master file, they can check whether they are using the latest version of the master file.

<table>
<thead>
<tr>
<th>Control type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Overflow</td>
<td>Overflow can occur if a field for computation is not initiated to zero at start. Some error in computation occurs, or unexpected high values occur.</td>
</tr>
<tr>
<td>b) Run –to- Run Control</td>
<td>In a tape based system, the processing of transaction file may involve several runs. For instance, a tape based order processing system might have a transaction tape that is used to update first a Stock Master File, then Sales Ledger, followed by general ledger. Various control totals may be passed from one run to the next, as a check on completeness of processing.</td>
</tr>
<tr>
<td>c) Cross Footing</td>
<td>Separate control totals can be developed for related fields and cross footed at the end of a run.</td>
</tr>
<tr>
<td>d) Range</td>
<td>An allowable value range can apply to a field</td>
</tr>
<tr>
<td>e) Sign Test</td>
<td>The contents of one record type field might determine which sign is valid for a numeric field.</td>
</tr>
</tbody>
</table>

13. WRITE SHORT NOTES ON PROCESSING CONTROLS IN A CIS ENVIRONMENT

1. Processing Controls are essential to ensure the integrity of data when input data is processed through multiple steps.
2. Processing Validation Checks primarily ensure that computation performed on numeric fields are authorized, accurate, and complete.
3. The following validation checks may be used –

<table>
<thead>
<tr>
<th>Control type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Overflow</td>
<td>Overflow can occur if a field for computation is not initiated to zero at start. Some error in computation occurs, or unexpected high values occur.</td>
</tr>
<tr>
<td>b) Run –to- Run Control</td>
<td>In a tape based system, the processing of transaction file may involve several runs. For instance, a tape based order processing system might have a transaction tape that is used to update first a Stock Master File, then Sales Ledger, followed by general ledger. Various control totals may be passed from one run to the next, as a check on completeness of processing.</td>
</tr>
<tr>
<td>c) Cross Footing</td>
<td>Separate control totals can be developed for related fields and cross footed at the end of a run.</td>
</tr>
<tr>
<td>d) Range</td>
<td>An allowable value range can apply to a field</td>
</tr>
<tr>
<td>e) Sign Test</td>
<td>The contents of one record type field might determine which sign is valid for a numeric field.</td>
</tr>
</tbody>
</table>

14. WRITE SHORT NOTES ON OUTPUT CONTROLS IN A CIS ENVIRONMENT

1. Output Controls ensure that the results of data processing are accurate, complete and are directed to the authorized recipient only.
2. The Auditor should examine whether audit trail relating to output was provided, and see the date and time when the output was so provided. This would enable the Auditor to identify the consequences of any errors discovered in the output.
Recording Controls enable records to be kept free of errors and transaction details that are input into the system.

1. **ERROR LOG:**
   a) Many of the accuracy checks can only be carried to during run time processing. So, it is important that a detected error does not bring the run to a halt.
   b) Hence, on discovery, the erroneous transaction is written to an error log file, which is examined at the end of the processing run.
   c) The identified errors can then be corrected or investigated with the relevant department before being input and processed further.
   d) This is important in batch entry and batch processing system.

2. **TRANSACTION LOG:**
   a) The transaction log provides a record of all transactions entered into the system, as well as storing transaction details such as Transaction Reference Number, Date, Account Number, Type of Transaction, Amount and Debit and Credit References.
   b) The Transaction will be stamped with details of input. These typically include Input Time, Input Date, Input Day, Terminal Number and User Number.
   c) It is used for multi – access mainframe system accounting transactions.
   d) Transaction Log can form the basis of an audit trail, and may be printed out for investigation during an audit. *(repeated login tries)*

16. **DOCUMENTATION CONTROLS IN CIS ENVIRONMENT**

1. Systems and Programs as well as modifications thereto, must be adequately documented and properly approved before being used.
2. Documentation ordinarily includes the following items –
   a) System Flowchart
   b) Program Flowchart
   c) Program Changes
   d) Operator Instructions
   e) Program Description (explaining the purpose for each part of the program.)

Adequate documentation evidencing approval of changes minimises the probability of unauthorized system and program changes that could result in loss of control and decreased reliability of financial data.

17. **WRITE SHORT NOTES ON STORAGE CONTROLS IN A CIS ENVIRONMENT.**

Storage Controls ensure the accurate, continuing and reliable storage of data. Since data is a vital resource for an organization and is the heart of CIS activities, special care must be taken to ensure the integrity of the Database or File System. The following types of Storage Controls may be used –

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Physical Protection against Erasure</td>
<td>a) Magnetic Tape Files have rings that may be inserted if the files are to be written or erased. Read only files have the ring removed.</td>
</tr>
<tr>
<td></td>
<td>b) Controls in respect of floppy Disks have a plastic lever, which is switched for read only purposes.</td>
</tr>
<tr>
<td>2. External labels</td>
<td>There are attached to tape Reels or Disk Packs, to identify the contents.</td>
</tr>
</tbody>
</table>
3. **Magnetic labels**

   a) External Labels are physical labels which are capable of being seen, but Magnetic Labels consists of magnetic machine-readable information encoded on the storage medium, which are used to identify its contents. File Header Labels appear at the start of a file and identify the file by name, give the date of last update and other information. This is checked by software prior to file updating.
   b) Trailer Labels at the end of files often contain control that are checked against those calculated during file processing.

4. **File Back-up Routines**

   Copies of important files are kept as backup, for security purposes. As the process of providing back-up often involves a computer operation in which one file is used to produce another, a fault in this process would have disastrous result (e.g. if both the master and the back-up were lost).

5. **Database back-up routines**

   a) The contents of a database held on a direct access storage device (DASD) such as magnetic disk is periodically dumped on to a back-up file.
   b) The back-up is usually a tape which is then stored together with the transaction log tape of all transactions occurring between the last and the current dump.
   c) If a fault in database, such as disk crash, happens afterwards, the state of the database can be recreated using the dumped data base tape, the stored transaction and the current log of transactions occurring between the previous dump and the time point of disk crash.

6. **Cryptographic Storage**

   a) Data is commonly written to files in a way that uses standard coding like ASCII or EBCDIC. It can be interpreted easily by unauthorized reader gaining access to the file.
   b) If the data is confidential or sensitive, then it may be scrambled prior to storage (coding) and unscrambled on reading (i.e. decoding).
   c) The security process involves the conversion of the plain text message or data into cipher text by the use of an encryption algorithm and an encryption key. The opposite process uses a decryption key to reproduce the plain text or message. If the encryption and decryption key are identical, the entire procedure is called Symmetric Cryptograph, otherwise, it is known as Asymmetric Cryptograph.

---

**18. USES / ROLE OF CAAT IN CIS ENVIRONMENT**

**Meaning:** CAATs are computer programs and data, that the auditor uses as part of audit procedures to process data of audit significance, contained in an entity’s information system. In a CIS environment, the application of auditing procedures may, require the Auditor to consider CAATs that use the computer as an audit tool, for enhancing the effectiveness and efficiency of audit procedures.

**Uses of CAATs:** CAATs may be used in performing various auditing procedures in the following:

1. Tests of details of transactions and balances, e.g. the use of audit software for recalculating interest, or extraction of invoices over a certain value from computer records.
2. Analytical Procedures, e.g. identifying inconsistencies or significant fluctuations,
3. Tests of general controls, e.g. 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 version approved by Management.
4. Sampling Programs to extract data for audit testing,
5. Tests of Application Controls, e.g. testing the functioning of a programmed control, and
6. Re-performing calculations performed by the entity’s accounting systems, e.g. depreciation, tax provisions, etc.,
7. CAATs are an efficient means of testing a large number of transactions or controls over large populations by
a) Analyzing and selecting samples from a large volume of transactions,
b) Applying analytical procedures, and
c) Performing substantive procedures

19. TYPES OF CAAT

❖ AUDIT SOFTWARE PROGRAMS
CAATs may consist of the following –

1. **Package Programs** are generalized computer programs designed to perform data processing functions, such as reading data, selecting and analysing information, performing calculations, creating data files and reporting in a format specified by the Auditor. **IDEA (reading lease terms / grouping them state wise / city wise as per pin codes / computing rent increase over period of time / comparing it with independent rent data from market / identifying exceptional items)**

2. **Purpose-Written Programs** perform audit tasks in specific circumstances. These programs may be developed by the Auditor, the entity being audited or an Outside Programmer hired by the Auditor. In some cases, the Auditor may use an Entity’s existing programs in their original or modified state, because it may be more efficient than developing independent programs. **(SONY assignment)**

3. **Utility Programs** are used by an entity to perform common data processing functions, such as sorting, creating and printing files. These programs are generally not designed for audit purposes, and therefore may not contain features such as automatic record counts or control totals. **(Features in accounting software)**

4. **System Management Programs** are enhanced productivity tools that are typically part of a sophisticated operating systems environment, for example, data retrieval software or code comparison software. As with utility programs these tools are not specifically designed for auditing use and their use requires additional care. **(Features in operating software)**

❖ **TEST DATA**
The Auditor enters a set of test data into the entity’s computer system and compares the results with predetermined results. /
Test data are used to test specific characteristics in compute* programs.
The test data are chosen by the Auditor.

**Test packs** It involves testing a set of data, chosen by the auditor, in the entity’s system, separately from the normal processing procedure.

**Integrated Test Facility** Here, auditor establishes a dummy unit to which test transactions are posted during the normal processing cycle of the entity. However, later on, the dummy entries should be eliminated from the entity’s accounting records. These are used mainly in case of On Line Real Time systems.

20. FACTORS TO BE CONSIDERED IN USE OF CAAT’S
When planning an audit, the auditor may consider an appropriate combination of manual and computer assisted audit technique, in determining whether to use CAATs. The Factors to be considered in this regard:

1. IMPRACTICABILITY OF MANUAL TESTS:
   a) Some audit procedures may not be possible to perform manually because they rely on computer processing (for e.g. advanced statistical analysis) or involve amounts of data that would overwhelm any manual procedure. *(comparing programme codes)*
   b) Further, many CIS programs perform tasks for which no hard copy evidence is available and, therefore, it may be impracticable for the Auditor to perform tests manually. The lack of hard copy evidence may occur at different stages in the business cycle. *(interest calculations are not printed.)* *(Analytical / Voluminous / No Hard Copies)*

2. AVAILABILITY OF CAATS AND SUITABLE COMPUTER FACILITIES/ DATA:
   a) The Auditor should consider the availability of CAATs, suitable computer facility and the necessary computer based information systems and data.
   b) The Auditor may plan to use other computer facilities when the use of CAATs on an Entities computer is uneconomical or impracticable. *(e.g. due to incompatibility between Auditor’s package program and Entity system)*
   c) Additionally, the Auditor, may choose to use new own facilities, such as PC’s or Laptops.
   d) Co-operation of Entity’s personnel is required, to provide processing facilities at a convenient time to assist with activities such as loading and running of CAAT on the Entity’s system, and to provide copies of data files in the format required by the Auditor. *(Compatible / Practical / Economical / Co-operation in facilities & time)*

3. IT KNOWLEDGE, EXPERTISE AND EXPERIENCE OF THE AUDIT TEAM: the audit team should have sufficient knowledge to plan, execute and use the resources of the particular CAAT adopted. The level of knowledge required depends on availability of CAATs and suitable computer facilities.

4. EFFECTIVENESS AND EFFICIENCY:
   The effectiveness and efficiency of auditing procedures may be improved by using CAATs to obtain and evaluate audit evidence. Matters relating to efficiency that an Auditor might consider include -
   a) Time taken to plan, design, execute and evaluate CAAT,
   b) Technical Review and Assistance hours,
   c) Designing and Printing of Forms (e.g. Confirmations), and
   d) Availability of Computer Resources.

5. TIME CONSTRAINTS:
   a) Certain data, such as transaction details are often kept for a short time and may not be available in machine-readable form by the time Auditor wants them. Thus, the auditor will need to make arrangement for the representation of data required, or may need to alter the timing of the work that requires such data.
   b) Where the time available to perform, an audit is limited, the auditor may plan to use CAAT, because its use will meet the auditor’s time requirement better than other possible procedures.

21. CONTROL PROCEDURE CAAT APPLICATIONS

1. CONTROL ASPECT: - The control aspect of CAAT application is achieved in two ways;
   a) Ensuring that reasonable detailed specifications of CAATs applied have been met, and
   b) The application of CAAT is not unduly manipulated by the entity’s staff.

2. FACTORS: - Specific procedures required to Control the use of a CAAT will depend on the particular application. The Auditor will have to consider the need to:
a) Approve technical specifications of the control,
b) Carry out a technical review of the work involving the use of CAAT,
c) Review the entity's general and specific IT Controls vouching the entity's integrity of the CAAT, and
d) Ensure appropriate integration of output with the audit process.

3. **CONTROL MEASURES**: The Auditor should take the following measures to control CAAT application-

<table>
<thead>
<tr>
<th>Control of Software Applications</th>
<th>Control of Test Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Participate in the design and testing of the computer programs.</td>
<td>a) Control the sequence of submission of less data to the system.</td>
</tr>
<tr>
<td>b) Check the coding of program to ensure conformity with detailed program pacifications.</td>
<td>b) Perform test runs containing small amounts of test data before submitting main audit test data.</td>
</tr>
<tr>
<td>c) Review of operating system instructions to ensure proper running of software in the entity's computer application.</td>
<td>c) Confirm that only current version programs are used to process test data.</td>
</tr>
<tr>
<td>d) Run audit software first on test files before taking up the same on main data files.</td>
<td>d) Predict the results of test data and compare with actual test data output, both for individual transactions and also in total.</td>
</tr>
<tr>
<td>e) Ensure use of correct files.</td>
<td>e) Obtain reasonable assurance regarding the continued use of current programs throughout the period of audit.</td>
</tr>
<tr>
<td>f) Obtain evidence as to implementation of audit software as planned.</td>
<td></td>
</tr>
<tr>
<td>g) Establish security measures to safeguard integrity and confidentiality of data. control CAAT applications.</td>
<td></td>
</tr>
</tbody>
</table>

4. **CONCURRENT AUDIT USING CAAT**: -

a) When the auditor intents procedures concurrently with online processing, the auditor should review those procedures with appropriate client personnel, and obtain approval before conducting the tests to help avoid the inadvertent corruption of client records.

b) To ensure appropriate control procedures, the presence of the Auditor is not necessarily required at the computer facility during the running of CAAT. It may, however, provide practical advantages, such as being able to control distribution of the output and ensuring the timely correction of errors, for example, if the wrong input file were to be used.

5. **OTHER MATTERS**: -

a) The Auditor requires the co-operation of the entity's staff that has an extensive knowledge of the entity's computer applications. However, he should ensure that the entity's staff do not manipulate with the CAAT or with the results of CAAT.

b) Though the presence of the Auditor is not required during the running of CAAT, his presence will ensure timely detection and correction of errors and also control distribution of test data output.