# 4

# Audit under Computerised Information System (CIS) Environment

Question 1

*How would the method of collecting audit evidence relating to effectiveness of controls and evaluating the same change under a computerized environment? (4 Marks, November, 2014)*

*Or*

*"The method of collecting Audit evidence and evaluating the same changes drastically under EDP Auditing". Comment. (8 Marks, November, 2007)*

Answer

Changes in Methods of Collecting and Evaluating the Audit Evidences in Computerised 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-

(i) Changes as 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:

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

(2) system development control include 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.

(ii) Changes as 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:

(1) whether a control is functioning reliably or multi functioning,

(2) 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 control are sufficient to maintain assets safeguarding, data integrity, system effectiveness and system efficiency and that they are in position and functioning.

## Question 2

*Write a short note on Causes of risk of material misstatement in CIS environment.*

*(4 Marks, May, 2014)*

## Answer

Causes of Risk of Material Misstatement in CIS Environment: In a CIS environment, the risk of a Material financial statement assertions being erroneously stated could arise from the deficiencies in the following cases -

(i) Program Development and maintenance.

(ii) System software support.

(iii) Operations including processing of data.

(iv) Physical CIS security.

(v) Control over access to specialized utility program.

## Question 3

*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.* *(4 Marks, November, 2013)*

Answer

Control Over Input transactions: Control are designed to provide reasonable assurance that-

(i) transactions are properly authorised before being processed by the computer.

(ii) transactions are accurately converted into machine readable from and recorded in the computer data files.

(iii) transaction are not lost, added, duplicated or improperly changed.

(iv) incorrect transactions are rejected, corrected and if necessary, resubmitted on a timely basis.

Control Over Output transactions: Designed to provide reasonable assurance that-

(i) results of processing are accurate.

(ii) access to output is restricted to authorised personnel.

(iii) output is provided to appropriate authorised personnel on a timely basis.

Question 4

*E & Co, a firm of Chartered Accountants, requires your help in identifying the audit procedures that can be performed using CAATs. Please guide them. (4 Marks, May, 2013)*

*Or*

*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. (6 Marks, May, 2012)*

Answer

Auditing Procedures Using CAATs: CAATs may be used in performing various auditing procedures, including the following-

(i) 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;

(ii) analytical procedures, for example, identifying inconsistencies or significant fluctuations;

(iii) tests of general 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 version approved by management;

(iv) sampling programs to extract data for audit testing;

(v) tests of application controls, for example, testing the functioning of a programmed control; and

(vi) Reperforming calculations performed by the entity's accounting systems.

Question 5

*What are the considerations which an auditor should consider while evaluating the reliability of the accounting and internal control systems in a CIS environment? (8 Marks, November, 2012)*

Answer

Consideration for Evaluating the Reliability of Accounting and Internal Control Systems in a CIS Environment: While evaluating the reliability of the accounting and internal control systems, the auditor would consider whether these systems-

(i) Ensure that authorized, correct and complete data is made available for processing;

(ii) Provide for timely detection and correction of errors;

(iii) Have Data recovery arrangement and Back-up system in place at all times;

(iv) Ensure that the case of interruption in the work of the CIS environment due to power, mechanical or processing failures, the system restarts without distorting the completion of the entries and records;

(v) Ensure the accuracy and completeness of output;

(vi) Provide adequate data security against fire and other calamities, wrong processing, frauds etc.;

(vii) Prevent unauthorized amendments to the program;

(viii) Provide for safe custody of source code of application software and data files.

Question 6

*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.*

*(5 Marks, November, 2011)*

Answer

Audit Plan for Evaluating the Reliability of Controls in CIS Environment: In evaluating the effects of a control, the auditor needs to assess the reliability by considering the various attributes of a control. Some of the attributes are- whether the control is in place and is functioning as desired, generality versus specificity of the 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-

(i) *Preventive controls:* Controls which stop errors or irregularities from occurring.

(ii) *Detective controls:* Controls which identify errors and irregularities after they occur.

(iii) *Corrective controls:* Controls which 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:

(i) Ensure that authorized, correct and complete data is made available for processing;

(ii) Provide for timely detection and correction of errors;

(iii) Ensure that the case of interruption in the work of the CIS environment due to power, mechanical or processing failures, the system restarts without distorting the completion of the entries and records;

(iv) Ensure that accuracy and completeness of output;

(v) Provide adequate data security against fire and other calamities, wrong processing, frauds etc.;

(vi) Prevent unauthorized amendments to the program;

(vii) Provide for safe custody of source code of application software and data files.

## Question 7

*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?*

*(4 Marks, May, 2011)*

## Answer

Risk Assessment: 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 ascertain being erroneously stated could arise from the deficiencies in the following case as-

(i) Program Development and maintenance.

(ii) System software support.

(iii) Operations including processing of data.

(iv) Physical CIS security.

(v) 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.

Question 8

*Different types of controls which operate over data moving into, through and out of the computer. Auditor is required to review such control. Comment. (8 Marks, November, 2010)*

Answer

The review process for controls in a Computerized Information System (CIS) Environment: In a CIS environment there are different types of control which operate over data moving into, through and out of the computer. 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 date entered. The review process can be laid down as follows-

(i) Organisation structure and control: The entity may have different functions under the CIS environment. There will be Date Administrator who will formulate data policies, plans the evaluation of the corporate data bases and maintain the data documentation. The data base administrator will be 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 and 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.

(ii) 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.

(iii) Access Control: The auditor has to ensure 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.

(iv) Input controls: The control in respect of input has to be effective to ensure that only properly authorized and approved data goes in the input into the CIS system. 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.

(v) Processing controls: These controls are must for integrity of data. Processing validation checks should be applied.

(vi) Recording Controls: This is for enabling the records to be kept free of errors.

(vii) Storage Controls: The data is the heart of the CIS system. Backup and recovery facilities will ensure the proper data availability to the management.

(viii) Output controls: The data processed must go to the authorized person in the manner it is required and for this purpose input controls are maintained. The auditor is interested to know whether the audit trail relating to output is provided.

Question 9

*The role of an auditor in collecting audit evidences under EDP system is more complex than under the manual system - Discuss. (8 Marks, November, 2009)*

Answer

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-

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

(ii) system development control include 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 softwares 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.

Question 10

*The auditor must evaluate major clauses of control used in a Computerised Information system to enhance its reliability – Comment. (8 Marks, November, 2008)*

Answer

Internal Controls in a CIS Environment: The reliability of a component is a function of control that acts on the component. In a computer system following are the major types of controls that are used to enhance component reliability which the auditor must evaluate-

(i) Authenticity Control: They are exercised to verify the identity of the individuals or process involved in a system (Password, digital signature etc.).

(ii) Accuracy Control: These attempts to ensure the correctness of the data and processes in a system (Programme validation check).

(iii) Completeness Control: This ensures that no data is missing and all processing is carried through to its proper conclusion.

(iv) Privacy Control: This ensures the protection of data from inadvertent or unauthorised disclosure.

(v) Audit Trail Controls: This ensures the traceability of all events occurred in a system.

(vi) Redundancy Control: It ensures that processing of data is done only once.

(vii) Existence Control: It attempts to ensure the ongoing availability of all system resources.

(viii) Asset safeguarding controls: It attempts to ensure that all resources within a system are protected from destruction or corruption.

(ix) Effectiveness Control: It attempts to ensure that the system achieves its goals.

(x) Efficiency Control: It attempts to ensure that a system uses minimum resources to achieve its goals.

Question 11

*Answer the following:*

*(a) "Use of Audit Software would increase the probability of detecting frauds". Comment.*

*(6 Marks, May, 2008)*

*(b) What is an Audit Trail? (4 Marks, May, 2008)*

Answer

(a) Use of Audit Software: CAATs allow the auditor to give access to data without dependence on the client, test the reliability of client software and perform audit tests more efficiently. CAATs are used to perform various audit procedures like-

(i) Tests of details of transactions and balances e.g. use of audits software to test all or a few transactions in a computer file.

(ii) Analytical review procedures e.g. use of audit software to identify unusual fluctuations or items.

(iii) Compliance tests of IT application controls e.g. use of test data to test the functioning of a programmed procedure.

However, the methods of applying audit procedures to gather evidence may be influenced by the methods of computer processing. Sometimes, in some accounting systems that use of computer for processing significant applications, it may difficult or impossible for an auditor to obtain certain data for inspection, inquiry or confirmation without computer assistance.

CAAT in Fraud Detection: In a CIS Environment, the Auditor is required to plan his work by exercising reasonable care and skill in such a manner that there is reasonable expectation of detecting material misstatements in the financial information resulting from fraud or error.

Use of the CAAT/ audit software systems will help the auditor to identify errors and frauds in the accounting and internal control system.

Conclusion: Frauds are intentional. Auditing through the computer with adequate knowledge of computer systems may highlight some frauds, but there is no empirical evidence to prove the assertion that the use of audit software systems has unearthed well concealed frauds.

Thus, it cannot be conclusively said that use of audit software systems increases the probability of detection of fraud.

(b) Audit Trail: Audit Trail can be defined as those documents, records, journals, ledgers, master files etc. that enables an auditor to trace the transactions from the source document to the summarised total in accounting reports or vice-versa.

Audit trail is the visible means whereby the auditor may have a business transactions through all the stages in which it features in the records of the business. For example, sequentially numbered sales invoice copies would normally be listed in a register or day book and subsequently filed either in numerical or chronological sequence. It would then be possible to trace a particular invoice from the day book to the original file or vice-versa by reference to the number or date of the invoice.

In a manual accounting system, it is possible to relate the recoding of a transaction at each successive stage enabling an auditor to locate and identify all documents from beginning to end for the purposes of examining documents, totalling and cross-totalling referencing.

However, in a CIS environment, the use of exception reporting by management has effectively eliminated the audit trail between input and output. Frequently computer generated totals, analysis and balances are not printed out in detail because the management is not exercising control through verification of the individual items processed.

Question 12

*Write a short note on Factors to consider in determining the use of Computer Assisted Audit Techniques (CAATs).* *(4 Marks, May, 2007)*

*Or*

*In determining whether to use Computer Assisted Auditing Techniques (CAATs), what are the factors that a statutory auditor has to consider?* *(6 Marks, May, 2005)*

Answer

Consideration of Factors in determining the use of CAATs:

(i) Availability of sufficient IT knowledge and expertise: It is essential that members of the audit team should possess sufficient knowledge and experience to plan, execute and use the results of CAAT. The audit team should have sufficient knowledge to plan, execute and use the results of the particular CAAT adopted.

(ii) Availability of CAATs and suitable computer facilities and data in suitable format: 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.

(iii) Impracticability of manual tests due to lack of evidence: Some audit procedures may not be possible to perform manually because they rely on complex processing (for example, advanced statistical analysis) or involve, amounts of data that would overwhelm any manual procedure.

(iv) Impact on effectiveness and efficiency in extracting a data: It includes selection of samples, applying analytical procedures, time involved in application of CAAT, etc.

(v) Time constraints in 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 arrangements for the retention of data required, or may need to alter the timing of the work that requires such data.

Question 13

*State the important characteristics of an effective system of Computer Audit Programme.*

*(8 Marks, November, 2006)*

*Or*

*State the important characteristics of an effective computer audit program system.*

*(8 Marks, May, 2004)*

Answer

Important Characteristics of an Effective System of Computer Audit Program: Normally, the computer audit program developed for general purposes shall have to customised according to needs of the organisation. However, an examination of following features is necessary to ensure that it is effective-

(i) Simplicity: The system should be simple to use and eliminate the need for remembering countless details normally required in writing or revising computer programs.

(ii) Understandability: The system should be readily understandable by 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.

(iii) 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.

(iv) 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. In addition, training provided for the audit staff is important. Also, maintenance service should be furnished, and provision made for future revisions in the programs.

(v) Statistical sampling capability: Since 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. In addition to simple random sampling and stratified sampling, it should have routines for more complex sampling such as cluster and multistage sampling.

(vi) Acceptability: The system should be acceptable to both the auditors and to computer centres. 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 be capable of minimum interference with normal routines.

(vii) Processing Capabilities: The package should be able to process many different types of applications. 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 the ability to operate under multiprogramming situations. It should have powerful, generalized audit commands.

(viii) 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.

Question 14

*Write a short note on Test Packs.* *(4 Marks, May, 2006)*

Answer

Test Packs: Test pack is a technique to determine the correctness of the computer programming used to record transactions through the computer. Preparation of test pack requires a great deal of expertise. It may be prepared by the auditor himself with the help of the entity's staff or by the Internal Control department of the entity. Normally test packs are used where-

(i) a significant part of the control system is embodied in the programme;

(ii) there are gaps in audit trail making it difficult to trace output from input and to verify intermediate calculation; and

(iii) the volume of records is large, so that it may be more economical and more effective to use test packs rather than to trace the transactions manually.

The operations of a test pack involve following steps:

(i) The auditor or the Internal Audit Department prepares a set of special data covering different types of transactions containing valid and unvalid conditions.

(ii) Data will include both that falling outside the control parameters (and printed out as an error or conception) and that falling within the parameters (and hence should be processed normally).

(iii) The test data are seen on the clients' computer with the client's programme but under audit supervision.

(iv) The results of the test data are also prepared separately, independent of the computer/programme, and are compared with the results obtained by running the programme through the computer.

(v) If the results are identical, reliability of the computer programme is proved.

Question 15

*Enumerate the risks and internal control characteristics in an audit conducted in Computer Information Systems (CIS) environment.* *(8 Marks, November, 2005)*

Answer

The Risks and Internal Control Characteristics in CIS Environment include the following:

(i) Lack of transaction trails: Some computer information systems are designed so that a complete transaction trail that is useful for audit purposes 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 (user) procedures.

(ii) Uniform processing of transactions: Computer processing uniformly processes like transactions with the same processing instructions. Thus, the clerical errors ordinarily associated with manual processing are virtually eliminated. Conversely, programming errors (or other systemic errors in hardware or software) will ordinarily result in all transactions being processed incorrectly.

(iii) 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. Thus, an individual who has access to computer programs, processing or data may be in a position to perform incompatible functions.

(iv) Potential for errors and irregularities: The potential for human error in the development, maintenance and execution of computer information systems may be greater than in manual systems, partially because of the level of detail inherent in these activities. Also, the potential for individuals to gain unauthorised access to data or to alter data without visible evidence may be greater in CIS than in manual systems.

In addition, decreased human involvement in handling transactions processed by computer information systems can reduce the potential for observing errors and irregularities. Errors or irregularities occurring during the design or modification of application programs or systems software can remain undetected for long periods of time.

(v) Initiation or execution of transactions: Computer information systems may include the capability to initiate or cause the execution of certain types of transactions, automatically. The authorisation of these transactions or procedures may not be documented in the same way as that in a manual system, and management's authorisation of these transactions may be implicit in its acceptance of the design of the computer information systems and subsequent modification.

(vi) 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. In turn, the effectiveness and consistent operation of transaction processing controls in computer applications is often dependent on the effectiveness of general computer information systems controls.

(vii) Potential for increased management supervision: Computer information systems can offer management a variety of analytical tools that may be used to review and supervise the operations of the entity. The availability of these analytical tools, if used, may serve to enhance the entire internal control structure.

(viii) Potential for the use of computer-assisted audit techniques: The case of processing and analysing large quantities of data using computers may require the auditor to apply general or specialised computer audit techniques and tools in the execution of audit tests.

Question 16

*Write a short note on Walk Through Tests.* *(4 Marks, May, 2005)*

Answer

Walk Through Tests: A walk-through is a procedure in which an auditor traces a transaction from its initiation through the company's information systems to the point when it is reflected in the financial reports. The auditor should perform one walk-through, at a minimum, for each major class of transactions. A walk-through provides evidence to confirm that the auditor understands (1) the process flow of transactions, (2) the design of identified controls for internal control components, including those related to preventing and detecting fraud, and (3) whether all points in the process have been identified at which misstatements related to relevant financial statement assertion could occur. Walk-throughs also provide evidence to evaluate the effectiveness of the controls' design and confirm that the controls have been placed in operation.

When performing a walk-through, the auditor should:

(i) Be sure that the walk-through encompasses the complete process (initiation, authorisation, recording, processing, and reporting) for each significant process identified, including controls intended to address fraud risk.

(ii) Ask the entity's personnel, at each of key stage in the process, about their understanding of what the company's prescribed procedures require.

(iii) Determine whether processing procedures are performed as expected on a timely basis, and look for any exceptions to prescribed procedures and controls.

(iv) Evaluate the quality of evidence provided and perform procedures that produce a level of evidence consistent with the auditor's objectives. The auditor should follow the whole process, using the same documents and technology that company staff use, asking questions of different personnel at each significant stage, and asking follow-up questions to identify any abuse of controls or fraud indicators.

Once a walk-through is performed, the auditor may carry forward the documentation, noting updates, unless significant changes make preparation of new documentation more efficient. If such significant changes occur in the process flow of transactions or supporting computer applications, the auditor should evaluate the nature of the changes and the effect on related accounts. The auditor should determine whether it is necessary to walk through transactions that were processed both before and after the change.

## Question 17

*(a) State the specific problems, which may arise in the implementation of internal control in an EDP system. (8 Marks, November, 2004)*

*(b) What are the characteristics of 'On-line Computer System'? (4 Marks, November, 2004)*

*(c) Explain: Tagging and Tracing. (4 Marks, November, 2004)*

## Answer

(a) Specific Problems of CIS relating to Internal Control: In a CIS environment, the following specific problems arise in the implementation of internal control-

(i) Separation 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.

(ii) 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 organisation identified a single user as the owner of the data.

(iii) 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 organisation, competent and trustworthy personnel is very much in demand. Unfortunately, the non availability of competent personnel, forced many organisation to compromise on their choice of staff. Moreover, it is not always easy for organisation 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.

(iv) System of Authorisation - Management authorisation of transaction may be either:

(1) general authorisation to establish policies for the organisation,

(2) specific authorisation applying to individual transactions. In manual system, auditors evaluate the adequacy of procedures for authorisation by examining the work of employees. In a computer system, authorisation 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 authorisation procedures, auditors have to examine not only the work of employees but also the veracity of the programme processing.

(v) 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.

(vi) 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 organisation does not have another suitable backup, it might be unable to continue operations.

(vii) 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 in 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 unauthorised actions.

(viii) 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 authorised 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.

(ix) 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 unauthorised 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.

(b) Characteristics of 'On-line Computer System': The characteristics of on-line computer systems may apply to a number of the types of on-line systems discussed in the previous section. The most significant characteristics relate to on-line data entry and validation, on-line access to the system by users, possible lack of visible transaction trail and potential programmer access to the system. The particular characteristics of a specific on-line system will depend on the design of that system.

(i) 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 the user to re-enter a valid part number.

(ii) On-Line Access: Users may have on-line access to the system that enables them to perform various functions, e.g., to enter transactions and to read, change or delete programs and data files through the terminal devices. Unlimited access to all of these functions in a particular application is undesirable because it provides the user with the potential ability to make unauthorised 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.

(iii) 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. However, the system may provide details of the transactions on request or through the use of transaction logs or other means. Illustrations of these types of systems include 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.

(iv) Programmer Access: Programmers may have on-line access to the system that enables them to develop new programs and modify existing programs. Unrestricted acess 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. For example, in some systems, programmers may have access only to programs maintained in a separate program development and maintenance library; whereas, in emergency situations which require changes to programs that are maintained on-line, programmers may be authorised to change the operational programs. In such cases, formal control procedurs would be followed subsequent to the emergency situation to ensure appropriate authorisation and documentation of the changes.

(c) Tagging and Tracing: It is a technique better than Integrated Test Data Facility. It involves tagging the client's input data in such a way that relevant information is displayed at key points. It uses the actual data, and so the question of elimination of 'special entries' test data designed under Integrated Test Data Facility does not arise. The hard copy, so produced is available only to the auditor and may describe such inputs as hours worked in a pay period in excess of 50; or sales orders processed in excess of ₹ 1,00,000. This enables the auditor to examine transactions at the intermediate steps in processing. The advantage of the tagging and tracing approach lies in the use of actual data and elimination of the need for reversing journal entries. The disadvantage is that the erroneous data will not necessary be tagged. An effective combination approach may be to use the ITF approach (integrated test facility) for a few hypothetical transactions and the tagging and tracing approach to follow line data through a complex system.