4

Audit under Computerised Information System (CIS) Environment

4.1 Introduction

Information Technology throughout the world has revolutionized and dramatically changed the manner in which the business is conducted today. Computerization has a significant effect on organization control, flow of document information processing and so on. Auditing in a CIS environment even though has not changed the fundamental nature of auditing, it has definitely caused substantial changes in the method of evidence collection and evaluation. This also requires auditors to become knowledge about computer environment (Hardware, software etc.) and keep pace with rapidly changing technology, even to the extent of using sophisticated Audit software. Students are advised to study the technical issue relating to Information Technology from the study material of paper 6.

4.2 Scope of Audit in a CIS Environment

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

(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.

(2) 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.

(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.

(4) Shifting of internal control base –

(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:

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:

a) authorisation, 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) 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.

(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 switch-over to computerised operations for ensuring performance quality standards.

(7) 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 selectivity provided.

(8) Man-machine interface / human-computer interaction - Man-machine interface ensures maximum effectiveness of the information system. Organisation 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.

4.3 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 from 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.

(2) From 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.

(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 us, destruction or substitution.

(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.

(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.

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 instance of the recent changes which the 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 Date 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 organisation.

(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.

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

(a) wide-spread end-user computing may result in unintentional errors creeping into systems owing to inept handling. Also coordinated program modification may not be possible.

(b) improper use of decision support system can have serious repercussion. Also their underlying assumption must be clearly documented.

(c) Usage of sophisticated audit software would be a necessity.

(d) Auditors non-participation at System Development Life Cycle State (SDLC) pose considerable problem in understanding the operational controls.

(e) Data communication and net working would introduce new audit risk.

(f) The move toward paperless EDI would eliminate much of the traditional audit trail radically changing the nature of audit trails.

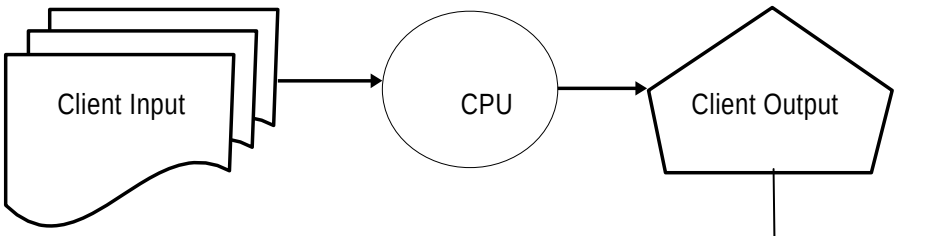
4.4 Audit Approach in a CIS Environment

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

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

B. A White-box approach i.e., Auditing through the computer.

A. The Black Box Approach



Auditing Around The Computer

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.

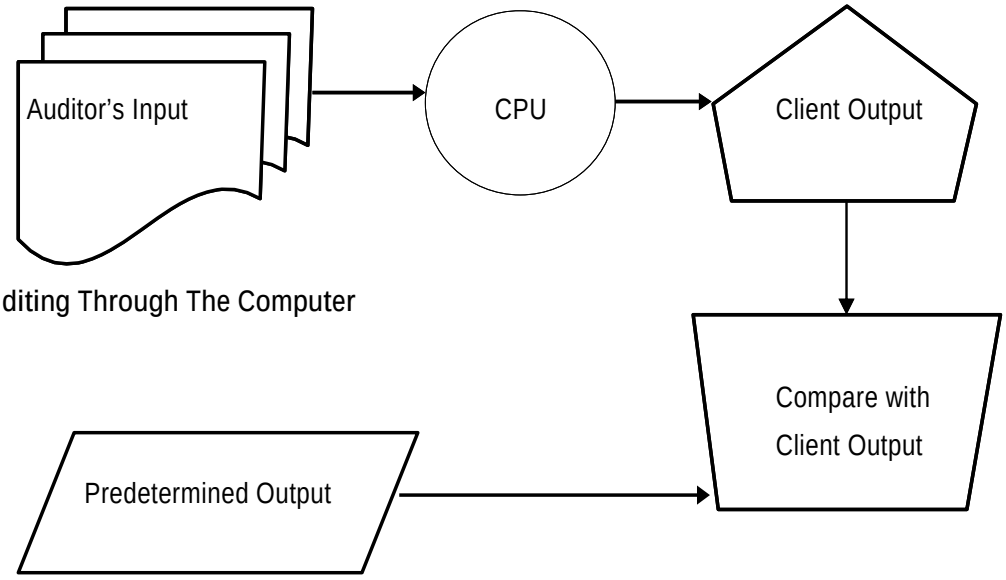
In testing, say, Payroll Application, the auditor might first examine selected time cards for hours worked and employee earning cards for rates and then trace these to the payroll summary output and finally compare hours, rates and extensions. The comparison of inputs and outputs may be done manually 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



Auditing Through The Computer

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:

(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 unauthorised access to the computer and the computerised database. The auditors task will also involve consideration of the separation of functions between staff involves in transaction processing and the computerised system and ensuring that adequate supervision of personnel is administered.

The process of auditing is not a straight forward 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 computerised 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.

4.5 Types of Computer Systems

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

A) System configuration, and

B) Processing systems.

A. Systems configuration

System configuration may be classified as:

(1) Large system computers - In large system computers, the processing task of multiple users is performed on a single centralised computer, i.e., all inputs move directly from the terminal to central processors and after processing goes back to users from central processors. All the terminals in these systems were called 'dumb terminals' as these terminals were not capable of processing data on their own and casually serve only as input/output terminals. With time, these systems have become more efficient and sophisticated. In many instances dumb terminals have given way to intelligent terminals i.e., allowing data processing at local levels.

(2) Stand alone personal computers - A stand alone system is one that is not connected to or does not communicate with another computer system. Computing is done by an individual

at a time. All input data and its processing takes place on the machine itself. Many small businesses rely on personal computers for all their accounting functions.

(3) Network computing system - A network is a group of interconnected system sharing services and interacting by a shared communication links. All networks have something to share, a transmission medium and rules for communication. Network share hardware and software resources. Hardware resources include:

(a) Client Server - A server in a network is dedicated to perform specific tasks to support other computers on the network. Common types of servers are:

(b) File Server - File servers are the network applications that store, retrieve and move data.

(c) Data base server - Most of the data base are client server based. Database servers provide a powerful facility to process data.

(d) Message Server - They provide a variety of communication methods which takes the form of graphics, digitized audio/video etc.,

(e) Print Server - Print server manages print services on the network.

Software resource sharing provides a facility to share information in the organisation.

The networks can also be classified on the basis of areas covered. Software resources include:

(1) Local area network - In a local area network (LAN), two or more computers located within a small well-defined area such as room, office or campus are connected through cables. One of the computers acts as the server, it stores the program and data files centrally. These programs and data files can be accessed by the other computers forming part of the LAN. LAN provides the additional advantage of sharing programs, data and physical resources like hard disks peripherals.

(2) Wide area network - Networks that employ public telecommunications facilities to provide users with access to the resources of centrally located computers. A WAN uses the public switched telephone network, high speed fibre optic cable, ratio links or the internet. When a LAN extends in the metropolitan area using the WAN technology, it is called Metropolitan Area Network (MAN).

WAN uses modem to connect computers over telephone lines (PSTN) PSTN system transfer analog signals. Therefore, public telephone system is not appropriate to connect computers. Modems are used to convert analog signals into digital and vice versa.

(3) Distributed data processing - The term has been used to cover many varities of computer system. It consists of hardware located at least two geographically distinct sites connected electronically by telecommunications where processing / data storage occur at two or more than one sites. The main computer and the decentralised units communicate via communication links. A more integrated connection occurs with 'cooperative processing where processing is handled by two cooperating geographically distinct processors. One processor send the output of its processing to another for completion. The system becomes more complex, where operating systems of both machines are different. Cooperative operating system may be required under such situation.

(4) Electronic data interchange (EDI) - EDI can be defined as:

The transfer of electronic data from one organisations computer system to another's, the data being structured in a commonly agreed format so that it is directly usable by the receiving organisation computer system.

EDI may be introduced where a group of organisations wish to ensure that electronic transactions are passed between one another. EDI groups require EDI services in order to effect the data exchanges. These are often provided by a third party in more than merely the transmission of the data. By providing these services the third party adds value to the data transmission and is thus called value added network (VAN). The following benefits accrue under EDI systems.

a) The speed with which an inter-organisational transaction is processed is minimised.

b) the paperwork involved in transaction processing is eliminated.

c) the costs of transaction processing are reduced, as much of the need for human interpretation and processing is removed.

d) reduced human involvement reduces error.

B. Processing system

Transaction processing systems include:

(1) Batch processing - Under batch processing a large volume of homologous transactions are aggregated and processed periodically. There are four steps in batch processing.

(a) Occurrence of transaction - The occurrence of business events is recorded in the source document.

(b) Recorded in a Transaction file - A batch of source is periodically transferred to the data entry operator to extract information from the source document and enter it into the computer format. Data entry is usually done off line. The computerised format is the transaction file to be processed in the system. Once the data entry is done, the records entered are confirmed with the source document. Once the records are checked, the source documents are stored separately for future reference.

(c) Updation of Master file - After all the data is entered in the system and it is processed and summarised, the master files are updated.

(d) Generation of output - After processing and master file updation, the report, as required are periodically generated.

Batch processing systems are used for processing large volumes of repetitive transactions where control considerations and efficient utilisation of computing capacity are important.

(2) On Line Processing System - One line processing refers to processing of individual transactions as they occur from their point of origin as opposed to accumulating them into batches. This is possible by direct access devices such as magnetic disk and number of terminals connected to and controlled by central processors. In this way, various departments in a company can be connected to the processor by cables.

Apart from transaction processing and file updating, inquires are also handled by the on-line processing system. On-line processing ensures that the records are in a updated status at any time whereas this is not so with batch processing, but the fact remains that online processing is costly.

(3) Interactive Processing - Under this processing mode, a continuous dialogue exists between the user and the computer. It is also called 'transaction driven' processing as transactions dealt with completely on an individual basis through all the relevant processing operations before dealing with the next transaction occur and enquiries to be dealt with on an immediate response basis.

(4) On-line real time processing - The term ' Real Time' refers to the technique of updating files with transaction data immediately after the occurrence of the event. Real time systems are basically on-line system with one speciality in enquiry processing. The response of the system to the enquiry itself is used to control the activity. The response of a real time system is one type of feed back control system. The response time would naturally differ from one activity to another. Real time system usually operates in multi-programming and multi-processing. This increases both availability and reliability of the system. CPU's in real time systems should possess the capability of 'Program Interrupts'. These are temporary stoppage of halts in the execution of a program so that more urgent message can be handled on priority. Some computer systems are dedicated to real time operations and others are designed to operate in both batch and real time modes so that they can also serve as stand by units to each other.

(5) Time Sharing - A time-sharing allows access to a CPU and files through many remote terminals. Multiprogramming is the method of implementing time shared operations. In transaction processing, time sharing occurs when a computer processes transactions of more than one entity.

(6) Service Bureau - A service bureau is a company that processes transaction for other entities. Such units may handle the computer processing for small companies that singly do not have sufficient transactions to justify the acquisition of a computer.

Advanced processing system further includes:

(a) Decision Support System - A Decision Support System (DSS) can be defined as a system that solving provided tools to managers to assist them in soloing semi-structured and an unstructured problem. A DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enables them to generate the information that is required by them for decision making. In other words, a DSS supports the human decision making process, rather then providing a means to replace it.

The decision-support system are characterised by:

(i) they support semi-structured or unstructured decision making

(ii) they are flexible enough to respond to the changing needs of decision makers, and,

(iii) they are easy to operate.

A decision-support system has 4 basic components:

(i) The Users – represent managers at any given level of authority in the organisation.

(ii) Data bases – contains both routine and non-routine data from both internal and external sources.

(iii) Planning Language – include general purpose planning language like spread sheets/special purpose planning languages, SAS, SPSS, Minilab etc;

(iv) Model Base – Model base is the 'Brain' of the decision support system because it perform data manipulations and computations with the data provided by the user and data base.

(b) Expert System - An expert system a computerised information system that allows non-experts to make decision comparable to that of an expert. Expert system are used for complex or ill structured tasks that require experience and special knowledge in specific subject areas.

As expert system typically contains

(i) Knowledge Base - This includes data, knowledge, relationships, rules of thumb to and decision rules used by experts to solve a particular type of problem. A knowledge base is the computer equivalent of all the knowledge and insight that an expert or a group of experts develop through years of experience in their field.

(ii) Inference Engine - This program contain the logic and reasoning mechanisms that stimulate the expert system logic process and deliver advice. It uses data obtained from both the knowledge base and the user to make associations and inference, forms its conclusion and recommends a course of action.

(iii) Use interface - This program allows the user to design, create, update, use and communicate with the expert system.

(iv) Explanation Facility - This facility provides the user with an explanation of the logic the expert system use to arrive.

(v) Knowledge acquisition Facility – Building a knowledge base (also called knowledge engineering), involves both a human expert and a know ledge engineer. The knowledge engineer is responsible for extracting an individuals expertise and using the knowledge acquisition facility to enter into the knowledge base.

(7) Integrated File System - These systems update many files simultaneously as transaction is processed. Processing of a sales order updates the accounts receivable control accounts and the related subsidiary ledger is also updated and the sales control and sales details are also posted as the sales order is processed.

Integrated data base system contains a set of interrelated master files that are integrated in order to reduce data redundancy. The software used to control input processing and output is referred to as Data Based Management System (DBMS) which handles the storage, retrieval, updating and maintenance of the data in the data base.

Integrated files are most commonly associated with OLRT (on-line real time) system and pose the greatest challenge to the Auditor's. Controls within these systems are harder to test and assess due to the danger of file destruction.

Files may be physically stored on disk in the following way:

'Sequentially' records are physically ordered by some field (e.g., employee number).

'Randomly' records are stored at a physical address computed by an algorithm working on a field value.

'Indexed' records are physically stored randomly with a sequentially ordered index field (e.g. by customer) and a pointer to the physical location of each record.

'Indexed Sequential' records are physically stored sequentially ordered by some field together with an index which provides access by some possibly other field.

If files are required to be processed sequentially, then they may be stored sequentially. The sequential update of an employee master file by time sheet data is an example. However, if individuals records are required to be accessed from time to time by some field e.g. employee name, then one of the other storage method may be used.

4.6 Effect of Computers on Internal Controls

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

(1) 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 creditors. 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.

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

(3) Competent And Trustworthy Personnel - Skilled, competent, well-trained and experienced in formation 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.

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

a) general authorisation to establish policies for the organisation,

b) 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.

(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 organisation 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 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.

(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 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.

(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 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.

4.7 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 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 focussed an cryptographic controls to project 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

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

4.8 Internal Controls in a CIS Environment

Internal control is an essential prerequisite for efficient and effective management of any organisation. Basically, they are the policies and procedure adopted by a management to achieve the entity's specific objectives like, physical verification of assets, periodic review and reconciliation of accounts, specific control on computer generated data etc.

An internal control is a CIS system depends on the same principal as that of manual system. Thus, the plan of organisation, delegation of powers, system authorisation, distribution of duties etc., are determined on similar consideration as in a manual system. However, in a CIS environment, due to difference in approach there is various other types of controls which are quite specific to CIS environment.

In setting up an internal control system in a CIS environment, the overall CIS operation need to be broken down into defined subsystem and controls established accordingly, addressing each function separately so that auditors can place reliance on them. The basic components that can be identified in a CIS environment are:

- Hardware (CPU, Monitor, Printers etc.)
- Software (Operating system, application programs, Data base management system etc.)
- People (Data entry operator, CIS organisation, end users)
- Transmission media

Once components have been identified, auditors must evaluate their reliability with respect to each type of error or irregularity that might occur.

The reliability of a component is a function of the controls that act on the component. A control is stated to be a set of activities designed to prevent, detect or correct errors or irregularities that affect the reliability of the components. The set of all control activities performed in a system constitutes the control subsystem within a system. Its function is to establish execute modify and maintain control activities so that the reliability of the system in maintained at an acceptable level. In a computer system many different types of controls are used to enhance component reliability. Major classes of control that the auditor must evaluate are:

(1) Authenticity Controls - Authenticity control are exercised to verify the identify of the individuals or process involved in a system (e.g. password control, personal identification numbers, digital signatures)

(2) Accuracy Control - Accuracy control ensure the correctness of data and processes in a system (e.g. program validation cheek that a numeric field contains only numeric, overflow checks, control totals, hash total etc.)

(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 attempts 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, inference control etc.)

(6) Audit Trail Controls - Audit trail control ensure 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) Asset 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.

4.9 Consideration of Control Attributes by the Auditors

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:

(1) whether the control is in place and is functioning as desired.

(2) 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.

(3) Whether the control acts to prevent, detect or correct errors.

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.

Auditors expect 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.

(4) The number of components used to execute the control.

Multi-component controls are more complex and more error prone but they are usually used to handle complex errors and irregularities.

4.10 Internal Control Requirement under CIS Environment

The requirement of internal control under CIS environment may cover the following aspects:

(1) Organisation And Management Control - Controls are designed to establish an organisational frame work for CIS activities including:

a) Policies and procedures relating to control functions.

b) Appropriate segregation of incompatible functions.

(2) Application System Development and Maintenance Control - Control are designed to provide reasonable assurance that systems are developed and maintained in an authorised and efficient manner, to establish control over:

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

b) changes made to application system.

c) access to system documentation.

d) acquisition of application system from third parties.

(3) Computer Operation Controls - Designed to control the operation of the system and to provide reasonable assurance that:

a) the systems are used for authorised purposes only.

b) access to computer operation is restricted to authorised personnel.

c) only authorised programs are to be used.

d) processing errors are detected and corrected.

(4) System Software Control - Controls are designed to provide reasonable assurance that system software is acquired or developed in an authorised and efficient manner including:

a) authorisation, approval, testing, implementation and documentation of new system software and system software modification.

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

(5) Data Entry And Program Control - Designed to provide assurance:

a) an authorisation structure is established over transaction being entered into the system.

b) access to data and program is restricted to authorised personnel.

(6) Control Over Input - Control are designed to provide reasonable assurance that:

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

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

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

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

(7) Control Over Processing and Computer Data Files - Controls are designed to provide reasonable assurance that:

a) transactions including system generated transactions are properly processed by the computer.

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

c) processing errors are identified and corrected on a timely basis.

(8) Control Over Output - Designed to provide reasonable assurance that

a) results of processing are accurate.

b) access to output is restricted to authorised personnel.

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

(9) Other Safeguards - Other safeguards include:

a) Offsite back-up of data and program.

b) Recovery procedures for use in the event of theft, loss or intentional or accidental destruction.

c) Provision of offsite processing in the event of disaster.

4.11 Approach to Auditing in a CIS Environment

Auditing in a computer Information System Environment emphasis that, the overall objective and scope of an audit do not change in a CIS environment. However, the use a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the entity.

The auditor should consider the effect of the factor like, (a) the extent of use of computers for preparing accounting information(c) efficacy of internal control over input, processing, analysis and reporting undertaken in the CIS installation and (c) the impact of computerisation on the audit trail that could otherwise be expected to exist in a manual system.

The approach to auditing in a CIS environment provides for the following:

(1) Skill and Competence - An auditor should have sufficient knowledge of the computer information systems to plan, direct, supervise control and review the work performed. The sufficiency of knowledge would depend on the nature and extent of the CIS environment. The auditor should consider whether any specialized CIS skills are needed in the conduct of the

audit. If the answer is in affirmative the auditor would seek the assistance of an expert possessing such skills.

(2) Planning - In regard to planning, 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.

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 procedures.

Auditors understanding the process would include -

a) The computer information systems infrastructure (hardware, operating system (s) and application software used by the entity, including changes therein since last audit, if any)

b) The 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.

c) Determination of the 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.

d) The auditor needs to determine extent of availability of data by reference to source documents, computer files and other evidential matters. Computer information systems may generate reports that might be useful in performing substantive tests (particularly analytical procedures). 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.

(3) Risk - When the computer information systems are significant the auditor should assess whether it may influence the assessment of inherent and control risks.

The nature of the risks and the ICS in CIS environment include the following:

(a) 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 procedures.

(b) Uniform processing of Transactions - Computer programs processing transactions uniformly, virtually eliminating the occurrence of clerical errors. However, if programming error exists all transactions will be processed incorrectly.

(c) Lack of Segregation of functions - Many controls becomes concentrated in a CIS environment allowing data processing of incompatible functions.

(d) 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, 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.

(e) Initiation or Execution of Transactions - In a CIS process certain types of transactions are triggered internally by the system, the authorization for which may not be documented as in manual system. In such cases, management; authorization of these transactions may be implicit.

(f) Dependence of Other Controls over Computer Processing - Certain manual control procedures are dependent on computer generated reports and outputs for their effectiveness. In term, the effectiveness and consistency of transaction processing controls are dependent on the effectiveness of general computer information systems controls.

(g) Increased management Supervision - Computer information can offer management a variety of analytical tools that can enhance the effectiveness of the entire internal control structure.

(h) Use of Computer - Assisted Audit Techniques - The Auditor may apply general or specialized computer audit techniques and tools in the execution of audit tests.

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) 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 complection 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.

(4) 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.

Risk may result from deficiencies in,

(a) Program development and maintenance,

(b) System software support;

(c) Operations

(d) Physical CIS security;

(e) Control over access to specialized utility programs;

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

Risk may also increase the potential for errors or fraudulent activities in;

(a) Specific applications.

(b) Specific data base or master files, or

(c) Specific processing activities.

As new CIS technologies are emerging for data processing and Clients are adopting the same for building complex computer systems, these may increase risk which needs further consideration

(5) Documentation - The Auditor should document the audit plan, the nature, timing and extent of audit procedures performed and the conclusions drawn from the evidence obtained. 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.

4.12 Review of Checks and Controls in a CIS Environment

General controls in a CIS environment falls under the three basic control approaches as seen under manual system, i.e. Feedback, feed-forward and preventive control. Apart from the three - fold categorization computer based information system also required different controls, though the emphasis is on preventive controls, Controls are present over many aspects of the computer system and its surrounding social environment. They operate over data moving into, through and out of the computer to ensure correct, complete and reliable processing and storage. There are other controls present over staff, staff involvement with the computer and access to data. Further controls are effective at preventing deterioration or collapse of the entire computing function.

Erroneous data processing by a computer system is likely to be the result of incorrect data input. This is the major point at which the human interfaces with the machine and it is here where important controls are placed.

Review Process -

(1) Organization Structure / Control - CIS function in an organization need to be so organized that different groups are formed to perform different duties in a large CIS installation. Some of the typical function that must be performed by select group includes:

(a) Data Administrator - Generates the data requirements of the users of information system services: formulates data policies, plans the evaluation of the Corporate data bases, maintains data documentation.

(b) Database Administrator - Responsible for the operational efficiency of corporate database, assist users to use database better.

(c) System Analyst - Manages information requirement for new and existing applications, designs information systems architectures to meet these requirements, facilitates implementation of information systems, writes procedures and users documentation.

(d) System Programmers - Maintains and enhances operating systems software, network software, library software, and utility software, provides when unusual systems failure occurs.

(e) Application Programmer - Designs programs to meet information requirements, codes, tests and debugs programs documents programs, modify program to remove errors, improve efficiency.

(f) Operation Specialist - Plans and control day-to-day operations, monitors and improves operational efficiency along with capacity planning.

(g) Librarian - Maintains library of magnetic media and documentation.

Auditors should be concerned about two matters:

i) Responsibilities of each job position must be clear; and incumbents must fully understand their duties, authority and responsibilities.

ii) The jobs performed within the information system function should maintain separation of duties to the extent possible. Without separation of duties, errors and irregularities might remain undetected.

(2) Documentation Control - Systems and programs as well as modifications, must be adequately documented and properly approved before being used: Documentation ordinarily assumes the following form:

a) A system flowchart;

b) A program flowchart;

c) Program change;

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.

(3) Access Control - Access controls are usually aimed at for preventing unauthorized access. The controls may seek to prevent persons who are authorised for access from accessing restricted data and program, as well as preventing unauthorized persons from gaining access to the system as a whole.

(a) Segregation Controls

- Access to program documentation should be limited to those persons who require it in the performance of their duties.
- Access to data files and programs should be limited to those individuals authorized to process data.
- Access to computer hardware should be limited to authorized individuals (e.g. Computer operators).

(b) Limited Physical Access to the computer Facility

- The physical facilities that hold the computer equipment, files and documentation should have controls to limit access only to authorized individuals.
- Types of controls may include, (a) using a guard, (b) automated key cards, (c) manual key locks, (d) new access devices like, fingerprints, palm prints, or other biometric devices.

(c) Visitor entry Logs - Entry logs should be uses to determine and documents those who have had access to the area.

(d) Hardware and Software access controls - Access control software like 'user identification' may be used. User identification is a frequently used control and is a combination of a unique identification code and a confidential password.

(e) Call back - It is a specialized form of user identification in which the user dials the system, identifies him and is disconnected from the system. Then, either an individual manually finds the authorized telephone number or the system automatically finds the authorized telephone number of the individual and finally the user is called back.

(f) Encryption - In encryption data is encoded when stored in computer files / and or before transmission to or from remote locations. This coding protects 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.

(g) Computer Application Controls - Programmed application controls apply to specific application rather than multiple applications.

These controls operate to assure the proper input and processing of data. The input steps converts human readable data into computer readable form. All CIS application are classified under 3 heads: Input, Processing and output.

(4) Input Controls - 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., Should perform editing of the data. Conversion of data into machine readable form should be controlled and verified for accuracy.

For validation of input controls, the following procedure can be applied:

(a) Pre-printed form - All constant information be printed on a source document. For example, if only limited number of responses to a question is considered appropriate then preprint the responses and have the user tick or circle the correct responses deleting those that are inappropriate.

(b) Check Digit - Errors made in transcribing and keying data can have serious consequences. One control used to guard against these types of errors is a 'Check Digit'.

A Check Digit is a redundant digit (s) added to a code that enables the accuracy of other characters in the code to be checked. The check digit can act as a prefix or suffix character or it can be placed somewhere in the middle of the code. When the code is entered, a program recalculates 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.

Calculation Of Check Digit

A simple way is to add the digits in a number and assign the result as a suffix.

Example: The number is 2148 the check digit is

2+1+4+8=15 i.e., 5 (dropping tens digit). The code is 21485

However, this does not protect transposition error, like 2814. The incorrect code will still produce the correct check digit.

This problem can be overcome by Module -11 test ; The Calculation steps are as under:

- The desired number = 2148.
- Make weighed average = 2x5 + 1x4 + 4x3 + 8x2 =42
- Divide by Modules 11 = 42/11 -3 with remainder 9
- Subtract the remainder from the modules = 11-9 =2 (check digit)
- Check digit is added as a suffix = 21482.

The check digit can be recalculated for verification as under:

- The encoded number = 21482
- Weighted average = (2x1)+(8x2)+(4x3)+(1x4)+(2x5) = 44.
- Division by the modules = 44/11 = 4 with no remainder.

If the remainder is zero, there is a high probability that the code is correct.

(c) Completeness Totals - To input data erroneously is one type error. To leave out or lose data completely is another type of error against which controls are provided.

(i) 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 made. For example, if a batch of invoices is to be imputed a total of all the invoices amounts might be calculated manually. 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. The method is not foot proof as compensating errors is possible.

(ii) Batch Hash Total - The idea is similar to control totals except that Hash totals are meaningless totals prepared purely for control purposes. The total of all customer account numbers in a batch is meaningless but may be used for control by comparing it with computer generated hash totals.

(iii) Batch Record Totals - Account is taken of the number of transactions and this is compared with the record count produced by the computer at the end of the batch.

(iv) 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.

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

(e) Field Checks - The following types of field checks may be applied:

(i) 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? Does the field contain blanks when data always should be present.

(ii) Alphabetic / Numeric - Does a field that should contain only alphabetic or numeric contain alphanumeric characters?

(iii) Range - Does the data for a field fall within its allowable value range?

(iv) 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?

(v) 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?

(vi) Format Mask - Data entered into a field might have to conform to a particular format, like 'yy mm dd'

(f) Record Checks - The following types of record checks can be applied:

(i) Reasonableness - Even though a field value might pass a range check, the contents of another field might determine what is a reasonable value for the field.

(ii) Valid-Sign-Numeric - The content of one field might determine which sign is valid for a numeric field.

(iii) 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.

(g) 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.

(5) Processing Controls - When input has been accepted by the computer, it usually is processed through multiple steps. Processing controls are essential to ensure the integrity of data. Almost all of the controls mentioned under input may also be incorporated during processing stage.

Processing validation checks primarily ensure that computation performed on numeric fields are authorized, accurate, and complete. The following validation checks may be indicated in this regard.

(i) Overflow - Overflow can occur if a field used for computation is not initiated to zero at

start. Some error in computation occurs, or unexpected high values occur.

(ii) Range - An allowable value range can apply to a field.

(iii) Sign Test - The contents of one record type field might determine which sign is valid for a numeric field.

(iv) Cross – Footing - Separate control totals can be developed for related fields and cross footed at the end of a run.

(v) Run-to-Run Control - 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 a sales ledger followed by a general ledger, various control totals may be passed from one run to the next as a check on completeness of processing.

(6) Recording Control - Recording controls enable records to be kept free of errors and transactions details that are input into the system.

(a) Error Log - This is particularly important in batch entry and batch processing system. Many of the accuracy checks can only be carried to during run time processing. It is important that a detected error does not bring the run to a halt, on discovery, the erroneous transaction is written to a error log file, which is examined at the end of processing. The errors can then be corrected or investigated with the relevant department before being input and processed.

(b) Transaction Log - The transaction log provides a record of all transactions entered into the system as well as storing transaction details such as the transaction reference number, the date, the account number, the type of transaction the amount and the debit and credit references. The transaction will be "Stamped" with details of input. These typically include input time, input date, input day, terminal number and user number. It is used for multi-access main frame systems accounting transactions. The transaction log can form the basis of an audit trail and may be printed out for investigation during an audit.

(7) Storage Control - These controls ensure the accurate and continuing and reliable storage of data. 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 controls are particularly accidental erasure of files and the precision of back-up and recovery facilities.

The following checks may be considered:

(a) Physical Protection Against Erasure - 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. The controls in respect of floppy disks have a plastic lever, which is switched for read only purposes.

(b) External Label - These are attached to tape reels or disk packs to identify the contents.

(c) Magnetic Labels - These consists of magnetic machine readable information encoded on the storage medium identifying 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 up dating. Trailer labels at the end of files often contain controls that are checked against those calculated during file processing.

(d) File Back - up Routines - Copies are held of important files 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 results; if both the master and the back-up were lost.

(e) Database Back - up routines - The contents of a data base held on a direct access storage device (DASD) such as magnetic disk are periodically dumped on to a back-up file. 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. If a fault in database, such as disk crash, happens afterwards the state of the data base can be recreated using the dumped data base tape, the stored transaction and the current log of transactions occurring between the dump and the crash point.

(f) Cryptographic Storage - 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. If the data is confidential or sensitive then it may be scrambled prior to storage and described on reading.

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 description 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.

(8) Output Control - Output control ensures that the results of data processing are accurate, complete and are directed to authorize recipient. The auditor should examine whether audit trail relating to output was provided and 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.

4.13 Computer Assisted Audit Techniques (CAATS)

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

Uses of CAATs - CAATs may be used in performing various auditing procedures, including the following:

- tests of details of transactions and balances, for example, the use of audit software for recalculating interest or the extraction of invoices over a certain value from computer records;
- analytical procedures, for example, identifying inconsistencies or significant fluctuations;

- 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 ;
- sampling programs to extract data for audit testing;
- tests of application controls, for example, testing the functioning of a programmed control; and
- reperforming calculations performed by the entity's accounting systems.

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 may consist of package programs, purpose-written programs, utility programs or system management program. a brief description of the programs commonly used is given below.

- Package Programs are generalized computer programs designed to perform data processing functions, such as reading data, selecting and analyzing information, performing calculations, creating data files and reporting in a format specified by the auditor.
- 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.
- 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.
- 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.

Considerations in the Use of Caats - When planning an audit, the auditor may consider an appropriate combination of manual and computer assisted audit techniques. in determining whether to use caats, the factors to consider include:

- the IT knowledge, expertise and experience of the audit team;
- the availability of CAATs and suitable computer facilities and data;
- the impracticability of manual tests;
- effectiveness and efficiency; and
- time constraints.

Before using caats the auditor considers the controls incorporated in the design of the entity's computer systems to which caat would be applied in order to determine whether, and if so, how, caats should be used.

It Knowledge, Expertise And Experience Of The Audit Team :Auditing in a computer information systems environment deals with the level of skill and competence the audit team needs to conduct an audit in a cis environment. It provides guidance when an auditor delegates work to assistants with cis skills or when the auditor uses work performed by other auditors or experts with such skills. specifically, the audit team should have sufficient knowledge to plan, execute and use the results of the particular caat adopted. the level of knowledge required depends on "availability of caats" and "suitable computer facilities".

Availability of CAATS and Suitable Computer Facilities - The auditor considers the availability of caats, suitable computer facilities and the necessary computer-based information systems and data. 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 program and entity's computer. Additionally, the auditor may elect to use their own facilities, such as pcs or laptops. The cooperation of the entity's personnel may be 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.

- Impracticability of Manual Tests - 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. In addition, many computer information systems 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.

Effectiveness and Efficiency - The effectiveness and efficiency of auditing procedures may be improved by using CAATs to obtain and evaluate audit evidence. CAATs are often an efficient means of testing a large number of transactions or controls over large populations by:

- analyzing and selecting samples from a large volume of transactions;
- applying analytical procedures; and
- performing substantive procedures.

Matters relating to efficiency that an auditor might consider include:

- the time taken to plan, design, execute and evaluate CAAT;
- technical review and assistance hours;
- designing and printing of forms (for example, confirmations); and
- availability of computer resources

In evaluating the effectiveness and efficiency of CAAT, the auditor considers the continuing use of CAAT application. The initial planning, design and development of CAAT will usually benefit audits in subsequent periods.

Time Constraints

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.

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.

Using CAATs -The major steps to be undertaken by the auditor in the application of CAAT are to:

(a) set the objective of CAAT application;

(b) determine the content and accessibility of the entity's files;

(c) identify the specific files or databases to be examined;

(d) understand the relationship between the data tables where a database is to be examined;

(e) define the specific tests or procedures and related transactions and balances affected;

(f) define the output requirements;

(g) arrange with the user and IT departments, if appropriate, for copies of the relevant files or database tables to be made at the appropriate cut off date and time;

(h) identify the personnel who may participate in the design and application of CAAT;

(i) refine the estimates of costs and benefits;

(j) ensure that the use of CAAT is properly controlled;

(k) arrange the administrative activities, including the necessary skills and computer facilities;

(l) reconcile data to be used for CAAT with the accounting and other records;

(m) execute CAAT application;

(n) evaluate the results;

(o) document CAATs to be used including objectives, high level flowcharts and run instructions; and

(p) assess the effect of changes to the programs/system on the use of CAAT.

Testing CAAT - The auditor should obtain reasonable assurance of the integrity, reliability, usefulness, and security of CAAT through appropriate planning, design, testing, processing and review of documentation. This should be done before reliance is placed upon CAAT. The nature, timing and extent of testing is dependent on the commercial availability and stability of CAAT.

Controlling CAAT Application - The specific procedures necessary to control the use of CAAT depend on the particular application. In establishing control, the auditor considers the need to:

(a) approve specifications and conduct a review of the work to be performed by CAAT;

(b) review the entity's general controls that may contribute to the integrity of CAAT, for example, controls over program changes and access to computer files. When such controls cannot be relied on to ensure the integrity of CAAT, the auditor may consider processing CAAT application at another suitable computer facility; and

(c) ensure appropriate integration of the output by the auditor into the audit process.

Procedures carried out by the auditor to control CAATs applications may include:

(a) participating in the design and testing of CAAT;

(b) checking, if applicable, the coding of the program to ensure that it conforms with the detailed program specifications;

(c) asking the entity's staff to review the operating system instructions to ensure that the software will run in the entity's computer installation;

(d) running the audit software on small test files before running it on the main data files;

(e) checking whether the correct files were used, for example, by checking external evidence, such as control totals maintained by the user, and that those files were complete;

(f) obtaining evidence that the audit software functioned as planned, for example, by reviewing output and control information; and

(g) establishing appropriate security measures to safeguard the integrity and confidentiality of the data.

When the auditor intends to perform audit procedures concurrently with online processing, the auditor reviews those procedures with appropriate client personnel and obtains approval before conducting the tests to help avoid the inadvertent corruption of client records.

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.