CHAPTER 4

Audit under Computerised Information System (CIS) Environment

Question 1

"Where the financial Accounting System has not been computerised, the auditor need not verify Computerised Management System ".

Answer

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

Question 2

What is an Audit Trail? Briefly describe the special audit techniques using the computer as an audit tool.

Answer

Audit Trail: Changes in hardware and software of data processing system have significantly changed the approach to auditing. The work of an auditor would be hardly affected if "audit trail" is maintained i.e. if it were still possible to relate, on a 'one-to-one' basis, the original input with the final output. In a manual accounting system, it is possible to relate the recording 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-referencing.

In first and early second-generation computer systems, a complete audit trail was generally available. However, with the advent of modern machines, the CIS environment has become more complex. This led to use of exception reporting by the management which effectively eliminated the audit trail between input and output. The lack of visible evidence may occur at different stages in the accounting process, for example:

(i) Input documents may be non-existent where sales orders are entered online. In addition, accounting transactions, such as discounts and interest calculations, may be generated by computer programmes with no visible authorisation of individual transactions.

(ii) The system may not produce a visible audit trail of transactions processed through the computer. Delivery notes and suppliers' invoices may be matched by a computer programme. In addition, programmed control procedures, such as checking customer credit limits, may provide visible evidence only on an exception basis. In such cases, there may be no visible evidence that all transactions have been processed.

(iii) Output reports may not be produced by the system. In addition, a printed report may only contain summary totals while supporting details are retained in computer files.

Special Audit Techniques: In the absence of audit trail, the auditor needs the assurance that the programmes are functioning correctly in respect of specific items by using special audit techniques. The absence of input documents or the lack of visible audit trail may require the use of Computer Assisted Audit Techniques (CAATs) i.e. using the computer as an audit tool. The effectiveness and efficiency of auditing procedures may be enhanced through the use of CAATs. Popularly, two common types of CAATs are in vogue, viz., test packs or test data and audit software or computer audit programmes. Normally speaking, special audit techniques may be used under the following circumstances:

(i) to ensure the correct functioning of important programme controls;

(ii) to overcome losses of audit trail;

(iii) to reduce audit costs or increase the efficiency of the audit.

Audit Software: Audit software consists of computer programmes used by the auditor, as part of his auditing procedures, to process data of audit significance from the entity's accounting system. It may consist of package programmes, purpose-written programmes, and utility programmes and systems management programs. Regardless of the source of the

programmes, the auditor should substantiate their validity for audit purposes prior to use.

- 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.

Test Data: Test data techniques are used in conducting audit procedures by entering data (e.g., a sample of transactions) into an entity's computer system, and comparing the results obtained with predetermined results. This enables to ascertain whether the controls residing in the hardware and in the programmes are operating correctly. Test data is used to test specific controls in computer programmes, such as online password and data access controls. Examples of such uses are:

(i) Test transactions selected from previously processed transactions or created by the auditor to test specific processing characteristics of an entity's computer system. Such transactions are generally processed separately from the entity's normal processing.

(ii) Test transactions in an integrated test facility where a "dummy" unit (e.g., a department or employee) is established and to which test transactions are posted during the normal processing cycle.

When test data is processed with the entity's normal processing, the auditor should ensure that the test transactions are subsequently eliminated from the entity's accounting records.

Question 3

A limited company having turnover of approximately ₹ 50 crores uses a tailor made accounting software package. In the said package, all transactions are recorded, processed and the final accounts generated from the system. The management tells you that in view of the voluminous nature of day books, there is no need to print them and that audit can be conducted on the computer itself. The management further assures you that any 'query based

reports' as required can be generated and printed. As a statutory auditor of the company, enumerate the procedures you would adopt to conduct the audit.

Answer

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

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

(i) operating accurately;

(ii) printing out all the exceptions which exist; and

(iii) bound by programmed control parameters which meet the company's genuine internal control requirements.

In view of the above, whether management relies upon exception reports, it effectively eliminated the audit trail between input and output and the auditor is forced to test the invisible processes which purport to embody the controls, and produce the output such as it is. These tests, which invariably involve the use by the auditor of the computer itself, are known as tests through the machine. In the 'through the machine' approach, the auditor starts by proving the accuracy of the input data, and then thoroughly examines (by applying tests) the processing procedures with a view to establishing the following that:

(i) all input is actually entered into the computer.

(ii) neither the computer nor the operators can cause undetected irregularities in the final reports.

(iii) the programmes appear, on the evidence of rejection and exception routines, to be functioning correctly.

(iv) all operator intervention during processing is logged and scrutinised by the DP manager.

The auditor in such circumstances will have to first evaluate the existing controls. For the same, he has to do the following:

(i) Evaluate the internal control system especially the controls and checks existing for recording the transactions, i.e., he has to verify at what level transactions can be entered into the system and what checks are available to prevent any unauthorised data entry and for rectifying errors/omissions in the transactions entered.

(ii) Evaluate at what level there is authority given for modification of transactions already entered. Is there any authority given only to a senior employee to carry out modifications? Or is it that once transactions are entered and validated no further modifications are possible thereto.

(iii) Whether there is a provision in the software for carrying out an on line audit of transactions, i.e. whether there a separate module in the package, where a separate password given to the auditor and once he has seen and approved a particular transaction/set of transactions, the same would be locked and no modifications would be possible by anyone (including the senior most employee) in the company.

(iv) Whether there are proper procedures for backup of data on a regular basis and whether the said procedures are being strictly followed.

(v) In case of any loss of data whether there is a clear defined recovery procedure to minimize the loss of data due to power failures or any human errors.

(vi) The auditor may introduce some dummy data into the system and see the results obtained.

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

(i) To check whether proper classification is done for revenue/capital - a report can be obtained of all purchases (not being raw materials or other routine purchases) exceeding ₹ one lakh.

(ii) To check whether all freight outward bills are accounted for a report containing a month-wise co-relation between goods dispatched and freight amount paid. The same can be further co-related with the freight rates obtained from the bills.

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

Question 4

"On-line real time processing system and batch processing system have their inherent strengths and weaknesses." Please comment.

Answer

On-line Real Time Processing System vs. Batch Processing System In an on-line real-time (OLRT) processing system, transactions are entered as they occur, and are processed as they are entered. These systems form the heart of management information systems. Given the continuous updating of the database as transactions are entered, the status of such files as accounts receivable, accounts payable, and inventory may be determined at any time. :. In an on-line real-time processing system, individual transactions are entered at terminal devices, validated and used to update related computer files immediately. An example is the application of cash receipts directly to customers' accounts. The results of such processing are then available immediately for inquiries or reports.

In a system with on-line batch processing, individual transactions are entered at a terminal device, subjected to certain validation checks and added to a transaction file that contains other transactions entered during the period. Later, during a subsequent processing cycle, the transaction file may be validated further and then used to update the relevant master-file. For example, journal entries may be entered master-file being updated on a monthly basis. Inquiries of, or reports generated from, the master-file will not include transactions entered after the last master-file update. In a batch processing system which is not on-line, transactions are accumulated and processed in group sales orders for the day, invoices to be recorded, and daily cash receipts might each be viewed as a "batch" of transactions, to be processed as a group. Batch processing systems are distinguished by their relative simplicity and reliability. They do not process transactions as quickly as the more advanced systems, nor do they possess the potential for providing timely information concerning the files updated by transactions processing. Given these limitations, the use of networked PCs terminals has become widespread, even among small entities. Batch processing systems are rarely found in today's systems environment.

Although powerful in terms of information capability, OLRT systems are more complex than batch processing systems. Moreover, they ordinarily do not provide the extent of audit trail documentation produced by batch system and for this they are more difficult to audit in terms of obtaining satisfaction concerning the existence of necessary controls, and of designing substantive testing procedures.

Conversely, in a batch processing system, the transaction are accumulated and processed in batches or groups. Control totals, both monetary and documentary, are also available for review to ensure completeness and accuracy of data being processed. The system is simple and reliable. However, its deficiency lies in the MIS is not updated on a concurrent basis and, therefore, information is not available on a timely basis.

Accordingly, it is a question of cost-benefit analysis as to which system will be more preferable to an entity.

Question 5

Indicate the control procedures which the auditor should adopt in applying CAAT (Computer Assisted Audit Technique) in an audit under CIS environment.

Answer

Computer Assisted Auditing Techniques (CAATs) involve performing audit procedures while conducting audit through the computer. Audit software and Test Data are two common type of CAATs. Using CAATs involves taking various measures including monitoring so that the use of CAATs by the auditor provides reasonable assurance that the audit objectives and detailed specifications of CAATs have been met. It is to be seen that CAATs are not manipulated by staff of the entity. The specific procedures necessary to control the use of a CAATs will 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 using a CAAT, the auditor may require the cooperation of the entity's staff who have extensive knowledge of the computer installation. In such circumstances, the auditor should have reasonable assurance that the entity's staff did not improperly influence the results of the CAAT.

Question 6

Discuss some problems that will be encountered in CIS Environment in implementation of internal control.

Answer

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.

Question 7

State the important characteristics of an effective computer audit programme system.

Answer

Characteristics of an effective computer audit program system: 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:

1. *Simplicity:* The system should be simple to use and eliminate the need for remembering countless details normally required in writing or revising computer programs.
2. *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.
3. *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.
4. *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.
5. *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.
6. *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.

7. *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.

8. *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 8

What are the characteristics of 'On-line Computer System'?

Answer

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.

1. 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.

2. 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.

3. 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.

4. Programmers may have on-line access to the system that enables them to develop new programs and modify existing programs. Unrestricted access provides the programmer with the potential to make unauthorised changes to programs and obtain unauthorised access to other parts of the system. The extent of this access depends on the requirements of the system. 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 procedures would be followed subsequent to the emergency situation to ensure appropriate authorisation and documentation of the changes.

Question 9

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

Answer

Consideration of Factors in Use of CAATs: In determining whether to use CAATs, the auditor should consider the following factors:

1. *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.
2. *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.
3. *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.
4. *Impact on effectiveness and efficiency in extracting a data*: It includes selection of samples, applying analytical procedures, time involved in application of CAAT, etc.
5. 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 10

"The method of collecting Audit evidence and evaluating the same changes drastically under CIS Environment". Comment on the above.

Answer

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 focused a 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.

Question 11

The auditor must evaluate major clauses of control used in a Computerised Information system to enhance its reliability – Comment.

Answer

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

1. *Authenticity Contro*l: They are exercised to verify the identity of the individuals or process involved in a system. (Pass word, digital signature etc.)
2. *Accuracy Control*: These attempts to ensure the correctness of the data and processes in a system (Programme validation check).
3. *Completeness Control*: This ensures that no data is missing and all processing is carried through to its proper conclusion.
4. *Privacy Control*: This ensures the protection of data from inadvertent or unauthorised disclosure.
5. *Audit Trail Controls*: This ensures the traceability of all events occurred in a system.
6. *Redundancy Control*: It ensures that processing of data is done only once.
7. *Existence Control:* It attempts to ensure the on going availability of all system resources.
8. *Asset safeguarding controls:* It attempts to ensure that all resources within a system are protected from destruction or corruption.
9. *Effectiveness Control*: It attempts to ensure that the system achieves its goals.
10. *Efficiency Control*: It attempts to ensure that a system uses minimum resources to achieve its goals.

Question 12

The role of an auditor in collecting audit evidences under EDP system is more complex than under the manual system - Discuss.

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:

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

Question 13

Different types of controls which operate over date moving into, through and out of the computer. Auditor is required to review such control. Comment.

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 form the date entered. The review process can be laid down as follows:

(1) 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.

(2) 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.

(3) 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.

(4) 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.

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

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

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

(8) 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 14

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?

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 15

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.

Answer

Auditing procedures using CAATs: CAATs may be used in performing various auditing procedures, including the following:

1. *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;*
2. *Analytical procedures, for example, identifying inconsistencies or significant fluctuations;*
3. *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 ;*
4. *Sampling programs to extract data for audit testing;*
5. *Tests of application controls, for example, testing the functioning of a programmed control; and*
6. *Re-performing calculations performed by the entity's accounting systems.*

Question 16

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.

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 for example are that 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

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

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

(3) 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.