

AUDIT UNDER COMPUTERISED INFORMATION SYSTEM (CIS) ENVIRONMENT

Question 1

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

Answer

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 is 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 controls are exercised to verify the identity of the individuals or process involved in a system (e.g. password control, personal identification numbers, digital signatures)
- (2) **Accuracy Control** - Accuracy controls ensure the correctness of data and processes in a system (e.g. program validation check that a numeric field contains only numeric, overflow checks, control totals, hash total etc.)
- (3) **Completeness Control** - Completeness controls attempt to ensure that no data is missing and that all processing is carried through to its proper conclusion. (e.g. program validation check, sequence check etc.)
- (4) **Redundancy Control** - Redundancy controls attempt to ensure that a data is processed only once. (e.g. batch cancellation stamp, circulating error files etc.)
- (5) **Privacy Controls** - Privacy controls ensure that data is protected from inadvertent or unauthorised disclosure. (e.g. cryptography, data compaction, inference control etc.)
- (6) **Audit Trail Controls** - Audit trail controls 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 availability 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.

Question 2

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

Answer

Changes to Evidence Collection - Collecting evidence on the reliability of a computer system is often more complex than collecting evidence on the reliability of a manual system. Auditors have to face a diverse and complex range of internal control technology that did not exist in manual system, like:

- 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 on cryptographic controls to protect the privacy of data. Unless auditors 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 3

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

Answer

The review process for controls in a computerized information system (CIS) environment.

In a CIS environment there are different types of control which operate over data moving into, through and out of the computer. These are designed in such a way that the correct, complete and reliable processing and storage is ensured. It is necessary for the auditor to review such controls in order to get the correct result from the data 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 Data 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 4

Z Ltd. has its entire operations including accounting computerized. As the audit partner you are concerned about inherent and control risk for material financial statement assertions. What could be the areas you look forward for deficiencies and risk identification? (4 Marks) (May 2011)

Answer

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

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

- (i) Program Development and maintenance.
- (ii) System software support.
- (iii) Operations including processing of data.
- (iv) Physical CIS security.
- (v) Control over access to specialized utility program.

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