


- Separation of Duties
 - Delegation of authority and responsibility
 - Competent and trustworthy personnel
 - System of Authorization
 - Adequate documents and records
 - Physical Control over assets and records
 - Adequate management supervision
 - Independent checks on performance
 - Comparing recorded accountability with assets
-

 **Separation of Duties:** It is a key control in an information system. Segregation basically means that the stages in the processing of a transaction are split between different people, such that one person cannot process a transaction through from start to finish. The various stages in the transaction cycle are spread between two or more individuals.


However, in a computerised system, the auditor should also be concerned with the segregation of duties within the IT department. Computer programs and data files cannot be changed without the use of computer equipment. When changes are made, however, there may be no visible evidence of the alteration. Thus, the organization of the information systems department should prevent its personnel from having inappropriate access to equipment, programs, or data files. This is accomplished by providing definite lines of authority and responsibility, segregation of functions, and clear definition of duties for each employee in the department.

 **Delegation of authority and responsibility:**

A clear line of authority and responsibility is an essential control in both manual and computer systems. May be difficult (in computer system) because some resources are shared among multiple users. When multiple users have access to the same data and the integrity of the data is somehow violated. Some attempted to overcome these problems by designing a single user as the owner of the data.

 **Competent and trustworthy personnel:**

The power vested in the personnel responsible for computer systems often exceeds the power vested in the personnel responsible for manual systems. Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task. In many countries across many years, well-trained and experienced IS personnel have been in short supply. Therefore, organizations sometimes have been forced to compromise in their choice of staff.

 **System of Authorization:** There must be some authorization procedure to ensure that transactions are approved. In some on-line transaction systems written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls

such as automated controls written into the computer programs (e.g. programmed credit limit approvals)

✚ **Adequate documents and records:** Record keeping is the controls over the protection and storage of documents, transaction details, and audit trails etc. The absence of a visible trail is not a problem for auditors, provided that systems have been designed to maintain a record of all events and the record can be easily accessed. Unfortunately, some software doesn't provide preservation of an accurate and complete audit trail. The obligation to maintain an audit trail exists in an IT environment just as it does in a manual setting. Audit trails may take form of pointers, hashing techniques, indexes, or embedded keys that link record fragments between and among database tables.

✚ **Physical Control over assets and records:** In the past manual systems could be protected from unauthorised access through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs are vulnerable to unauthorised amendment at the computer or from remote locations. The use of wide area networks, including the Internet, has increased the risk of unauthorised access. The nature and types of control available have changed to address these new risks.

✚ **Adequate management supervision:** Management's supervision and review helps to deter and detect both errors and fraud. In computer-based system, supervision needs to be carried out remotely. Managers must examine and do periodic auditing to check for unauthorized actions.

✚ **Independent checks on performance:** The control emphasis should be on ensuring the veracity of program code. Auditors must evaluate controls established for program development, modification, operation and maintenance.

✚ **Comparing recorded accountability with assets**

* * * * *