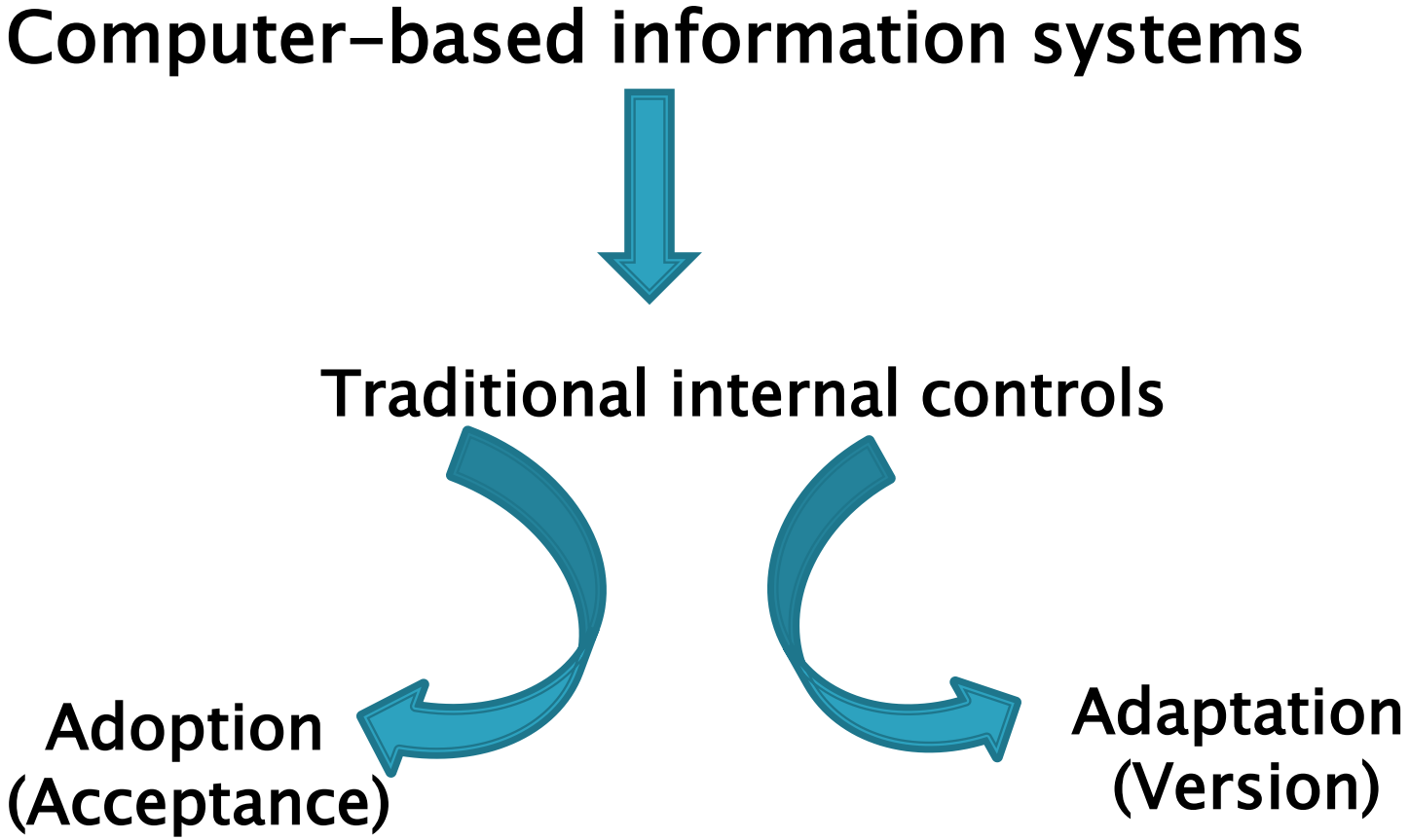
CHAPTER 1 Overview of Information Systems Auditing

EFFECTS OF COMPUTERS ON INTERNAL CONTROLS

- The goals of asset safeguarding, data integrity, system effectiveness, and system efficiency can be achieved only if an organization's management sets up a system of internal control.

Effects of Computer-based information systems on traditional internal controls



Major components of an internal control system

- Separation of duties
- Clear delegation of authority and responsibility
- Competent and Trustworthy Personnel/ Recruitment and training of high-quality personnel
- System of authorizations
- Adequate documents and records
- Physical control over assets and records
- Adequate management supervision
- Independent checks on performance
- Periodic comparison of recorded accountability with assets

Separation of Duties

- In a manual system, separate persons should be responsible for initiating transactions, recording transactions, and maintaining custody of assets.

- As a basic control, separation of duties prevents or detects errors and irregularities.

- In a computer system, however, the traditional notion of separation of duties does not always apply.

For example,

A program could reconcile a vendor invoice against a receiving document and print a check for the amount owed to a creditor.

Thus, the program is performing functions that in manual systems would be considered to be incompatible.

Nevertheless, it might be inefficient and, from a control viewpoint, useless to place these functions in separate programs.

- Instead, separation of duties must exist in a different form When it has been determined that the program executes correctly, the capability to run the program in production mode and the capability to change the program must be separated.

- In minicomputer and microcomputer environments, separation of incompatible functions could be even more difficult to achieve.

- Some minicomputers and microcomputers allow users to change programs and data easily.

- Furthermore, they might not provide a record of these changes. Thus, determining whether incompatible functions have been performed by system users can be a difficult or impossible.

Delegation of Authority and Responsibility

- A clear line of authority and responsibility is an essential control in both manual and computer systems.

- In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users.

For example, one objective of using a database 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 organizations have attempted to overcome these problems by designating a single user as the owner of the data. This user assumes ultimate responsibility for the integrity of the data.

Authority and responsibility lines have also been blurred by the rapid growth in end-user computing.

Because high-level languages are more readily available, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by information systems professionals.

Although these developments have substantial benefits for the users of computing services in an organization, unfortunately, they exacerbate the problems of exercising overall control over computing use.

Competent and Trustworthy Personnel

- Important power is often vested in the persons responsible for the computer based information systems developed, implemented, operated, and maintained within organizations.

For example, a systems analyst might be responsible for advising management on the suitability of high-cost, high-technology equipment.

Similarly, a computer operator, sometimes takes responsibility for safe guarding critical software and critical data during execution of or backup of a system.

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 and across many years, well-trained and experienced information systems **personnel have been in short supply.**

Therefore, organizations sometimes have been forced to compromise in **their choice of staff.**

Moreover, it is not always easy for organizations to assess the competence and integrity of their information systems staff.

High turnover among these staff has been the norm.

Therefore, managers have had insufficient time to evaluate them properly.

In addition, the rapid evolution of technology inhibits management's ability to evaluate an in formation systems employee's skills.

Some information systems personnel also seem to lack a well-developed sense of ethics, and some seem to delight in subverting controls.

System of Authorizations

- Management issues two types of authorizations to execute transactions.

1. General authorizations

2. Specific authorizations

First, **General authorizations** establish policies for the organization to follow.

For example, a fixed price list is issued for personnel to use when products are sold.

Second, **Specific authorizations** apply to individual transactions.

For example, acquisitions of major capital assets might have to be approved by the board of directors.

Adequate Documents and Records

- **In a manual system,** adequate documents and records are needed to provide an audit trail of activities within the system.

- **In computer systems,** documents might not be used to support the initiation, execution and recording of some transactions.

- **For examples,** in an online order-entry system, customers' orders received by telephone might be entered directly into the system.

Similarly, some transactions might be activated automatically by a computer system.

For example, an inventory replenishment program could initiate purchase orders when stock levels fall below a set amount.

Thus, no visible audit or management trail would be available to trace the transaction.

The absence of a visible audit 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.

In well-designed computer systems, audit trails are often **more extensive than** those maintained **in manual systems.**

Unfortunately, not all computer systems are well designed.

Some software, for example, does not provide adequate access controls and logging facilities to ensure preservation of an accurate and complete audit trail.

When this situation is coupled with a decreased ability to separate incompatible functions, serious control problems can arise.

Physical Control over Assets and Records

- Physical control over access to assets and records is critical in both manual systems and computer systems.

- **Computer systems** differ from manual systems, however, in the way they concentrate the information systems assets and records of an organization.

For example, in a **manual system**, a person wishing to perpetrate a fraud might need access to records that are maintained **at different physical locations.**

In a computer system, however, all the necessary records can be maintained **at a single site** namely, the site where the computer is located.

Thus, the perpetrator does not have to go to physically disparate locations to execute the fraud.

This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster.

For example, a fire that destroys a computer room could result in the loss of all major master files in an organization.

If the organization does not have suitable backup, it might be unable to continue operations.

Adequate Management Supervision

In a manual system, management supervision of employee activities is relatively straightforward because the managers and the employees are often at the same physical location.

In computer systems, data communications facilities can be used to enable employees to be closer to the customers they service.

Thus, supervision of employees 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 inquiry.

Computer systems also **make** the activities of employees less visible to management.

-----Because many activities are performed electronically, managers must periodically access the audit trail of employee activities and examine it for unauthorized actions.

Again, the effectiveness of observation and inquiry as controls is decreased.

Independent Checks on Performance

- In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures.

- Checks by an independent person help to detect any errors or irregularities.

If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like a 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 program code.

Insofar as many independent checks on performance are no longer appropriate, auditors must now evaluate the controls established for program development, modification, operation, and maintenance.

Comparing Recorded Accountability with Assets

Data and the assets that the data importance to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred.

In a manual system, independent staff prepare the basic data used for comparison purposes.

In a computer system, however, software is used to prepare this data.

For example, a program can be implemented to sort an inventory file by warehouse location and to prepare counts by inventory item at the different warehouses.

If unauthorized modifications occur to the program or the data files that the program uses, an irregularity might not be discovered.

For example, stealing of inventory from a particular warehouse bin.

Again, internal controls must be implemented to ensure the accuracy of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.


BEST OF LUCK