Chapter - 3
Conducting an Information Systems Audit

- Introduction
- Nature of Controls
- Audit Risks
- Types of Audit Procedures
- Steps in an Audit
- Auditing Around or Through the Computer

Introduction:

The Audit of an IS environment to evaluate the systems, practices and operations may include one or both of the following:

- Assessment of internal controls within the IS environment to assure validity, reliability, and security information.
- Assessment of the efficiency and effectiveness of the IS environment in economic terms.

The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole. This includes evaluating both the effectiveness and efficiency. The focus (scope and objective) of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness (result-orientation) and efficiency (optimum utilization of resources).

It is a sobering experience to be in charge of the information systems audit of an organization that has several hundred programmers and analysts, many computers, and thousands of files. Obviously, all organizations are not this size. Except for the smallest organizations, however, auditors usually cannot perform a detailed check of all the data processing carried out within the information systems function. Instead, they must rely on a sample of data to determine whether the objectives of information system auditing are being achieved.

So to obtain reasonable assurance that an organization safeguards its data-processing assets, maintains data integrity, and achieves system effectiveness and efficiency, the following steps becomes to be useful.

✓ We start by examining the nature of controls and discussing some techniques for simplifying and providing order to the complexity encountered when making evaluation judgments on computer-based information systems.

✓ Next we consider some of the basic risks auditors face, how these risks affect the overall approach to an audit and the types of audit procedures used to assess or control the level these risks.

✓ Finally, we examine a major decision auditors must make when planning and conducting an information systems audit namely, how much do they need to know about the internal workings of a computer-based information system before an effective audit can be conducted?

The Nature of Controls:

Objective of Controls

The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss. Exposures are potential losses due to threats materializing. All exposures have causes. Some categories of exposures are:

- ✓ Errors or omissions in data, procedure, processing, judgment and comparison.
- ✓ Improper authorizations and improper accountability with regards to procedures, processing, judgment and comparison.
- ✓ Inefficient activity in procedures, processing and comparison.
- ✓ Some of the critical control considerations in a computerized environment are:
- ✓ Lack of management understanding of IS risks and lack of necessary IS and related controls.
- ✓ Absence or inadequate IS control framework.
- ✓ Absence of or weak general controls and IS controls.
- ✓ Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff.
- ✓ Complexity of implementation of controls in distributed computing environments and extended enterprises.
- ✓ Lack of control features or their implementation in highly technology driven environments.
- ✓ Inappropriate technology implementations or inadequate security functionality in technologies implemented.

The control objectives serve two main purposes:

(i) Outline the policies of the organization as laid down by the management.

(ii) A benchmark for evaluating whether control objectives are met.

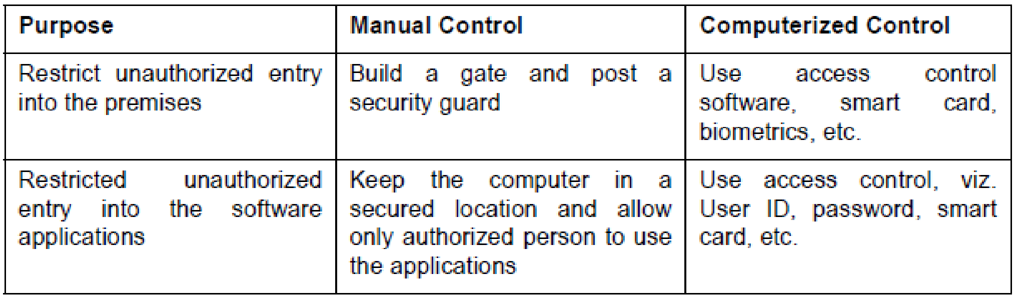
Information systems auditors ultimately are concerned with evaluating the reliability or operating effectiveness of controls. It is important, therefore, that we understand what is meant by a control. **"A control is a system that prevents, detects, or corrects unlawful events."** There are three key aspects to this definition.

First, a control is a system. In other words, it comprises a set of interrelated components that function together to achieve some overall purpose.

Second, the focus of controls is unlawful events. An unlawful event can arise if unauthorized inaccurate, incomplete, redundant, ineffective or inefficient input enters the system. **For example,** a data-entry clerk might key incomplete data into the system. An unlawful event can also arise if the system transforms the input in an unauthorized, inaccurate, incomplete, redundant, ineffective or inefficient way.

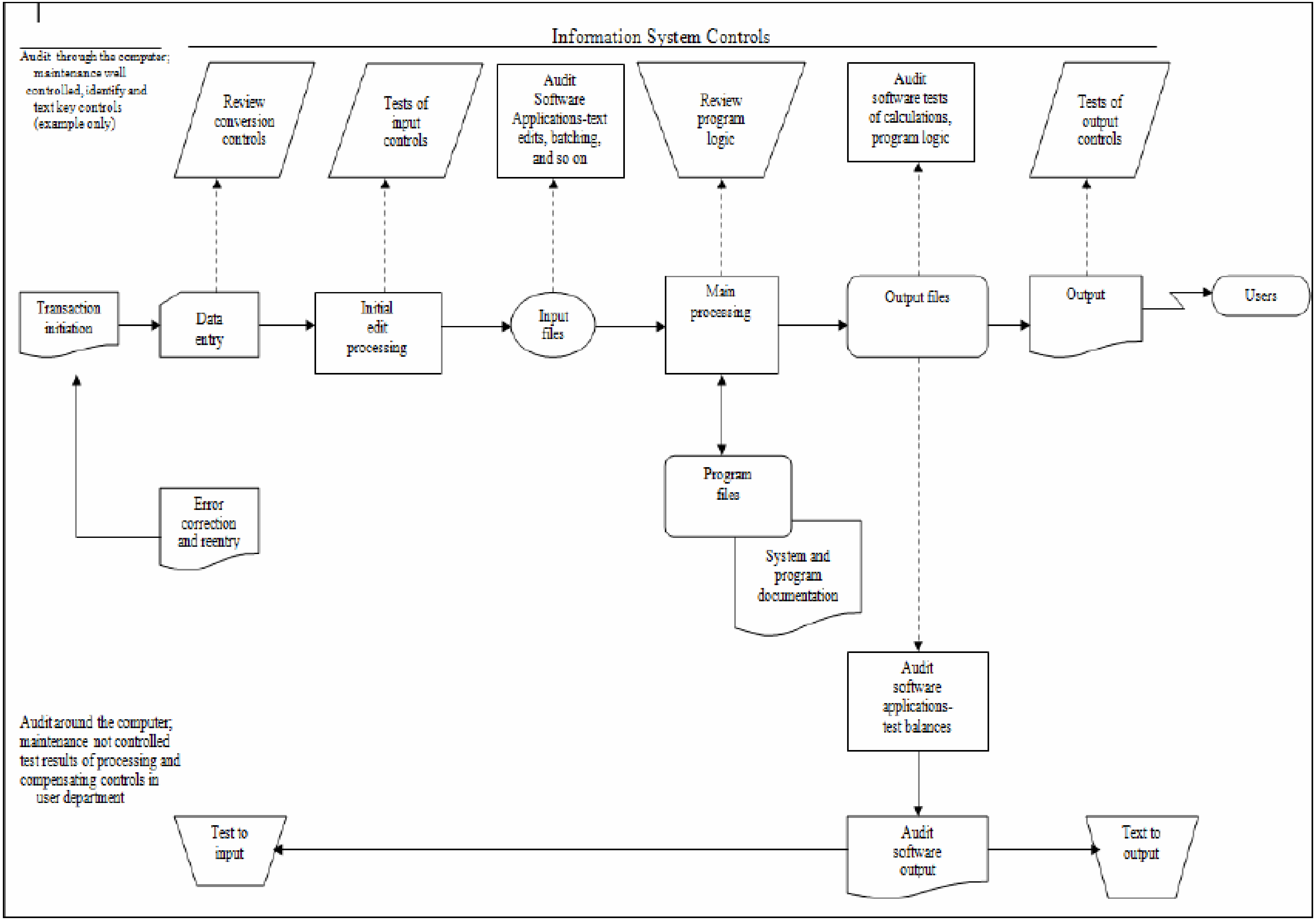
Third, controls are used to prevent, detect, or correct unlawful events. Consider some examples:

1. **Preventive control:** Instructions are placed on a source document to prevent clerks from filling it out incorrectly. Note that the control works only if the instructions are sufficiently clear and the clerk is sufficiently well trained to understand the instructions. Thus, both the clerk and the instructions are components of the system that constitutes the control. The instructions by themselves are not the control.



Purpose	Manual Control	Computerized Control
Restrict unauthorized entry into the premises	Build a gate and post a security guard	Use access control software, smart card, biometrics, etc.
Restricted unauthorized entry into the software applications	Keep the computer in a secured location and allow only authorized person to use the applications	Use access control, viz. User ID, password, smart card, etc.

Table 3.2 : Preventive Controls


Information System Controls
Audit through the computer; maintenance well controlled, identify and text key controls (example only)
Review conversion controls
Tests of input controls
Audit Software Applications-text edits, batching, and so on
Review program logic
Audit software tests of calculations, program logic
Tests of output controls
Transaction initiation
Data entry
Initial edit processing
Input files
Main processing
Output files
Output
Users
Error correction and reentry
Program files
System and program documentation
Audit software applications-test balances
Audit around the computer; maintenance not controlled test results of processing and compensating controls in user department
Test to input
Audit software output
Text to output

Examples of preventive controls

- Employ qualified personnel
- Segregation of duties
- Access control
- Documentation
- Prescribing appropriate books for a course
- Training and retraining of staff
- Authorization of transaction
- Validation, edit checks in the application
- Firewalls
- Anti-virus software
- Passwords

2. **Detective control:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An input program identifies incorrect data entered into a system via a terminal. Again, the control is a system because various parts of the program must work together to pinpoint errors.

Examples of detective controls include

- Hash totals
- Check points in production jobs
- Echo control in telecommunications
- Error message over tape labels
- Duplicate checking of calculations
- Periodic performance reporting with variances
- Past-due accounts report
- The internal audit functions
- Intrusion detection system
- Cash counts and bank reconciliation
- Monitoring expenditures against budgeted amount

Corrective control: Corrective controls are designed to reduce the impact or correct an error once it has been detected. A business continuity plan is considered to be a significant corrective control. A program uses special codes that enable it to correct data corrupted because of noise on a communications line. Once more, the control is a system because various parts of the program must work together in conjunction with the error-correcting codes to rectify the error.

Examples of Corrective Controls

- Contingency planning
- Backup procedure
- Rerun procedures
- Treatment procedures for a disease
- Change input value to an application system
- Investigate budget variance and report violations.

Audit risks:

We know that information systems auditors are concerned with four objectives: asset safeguarding, data integrity, system effectiveness and system efficiency.

Both external and internal auditors are concerned with whether errors or irregularities cause material losses to an organization or material misstatements in the financial information prepared by the organization. If you are an internal auditor, it is likely you will also be concerned with material losses that have occurred or might occur through ineffective or inefficient operations. External auditors, too, might be concerned when ineffective or inefficient operations threaten to undermine the organization. Moreover many external auditors report such problems as part of their professional services to the management of an organization.

To assess whether an organization achieves the asset safeguarding, data integrity, system effectiveness, and system efficiency objectives, auditors collect evidence. Because of the test nature of auditing, auditors might fail to detect real or potential material losses or account misstatements. **The risk of an auditor failing to detect actual or potential material losses or account misstatements at the conclusion of the audit is called the audit risk.** Auditors choose an audit approach and design audit procedures in an attempt to reduce this risk to a level deemed acceptable.

As a basis for determining the level of desired audit risk, some professional bodies of auditors have adopted the following audit risk model for the external audit function:

DAR= IR X CR X DR

In this model,

- ✓ **DAR** is the desired audit risk.
- ✓ **IR** is the inherent risk, which reflects the likelihood that a material loss or account misstatement exists in some segment of the audit before the reliability of internal controls is considered.
- ✓ **CR** is the control risk, which reflects the likelihood that internal controls in some segment of the audit will not prevent, detect, or correct material losses or account misstatements that arise.
- ✓ **DR** is the detection risk, which reflects that the audit procedures used in some segment of the audit will fail to detect material losses or account misstatements.

To apply the model, auditors first choose their level of **desired audit risk**. In addition, they assess the short and long-run consequences for their organizations if they fail to detect real or potential material losses from ineffective or inefficient operations.

Next auditors consider the level of inherent risk. Initially auditors consider general factors such as the nature of the organization (e.g. Is it a high flyer?), the nature of industry in which it operates (e.g. Is the industry subject to rapid change?), the characteristics of management (e.g. Is management aggressive and autocratic?). Auditors then consider the inherent risk associated with different segments of the audit.

To assess the level of control risk associated with a segment of the audit, auditors consider the reliability of both management & and application controls, Auditors Management controls constitute protective layers of "onion skins" around applications. Forces that erode asset safeguarding, data integrity, system effectiveness and system efficiency must penetrate each layer to undermine a lower layer. To the extent the outer layers of controls are intact the inner layers of controls are more likely to be intact.

Next auditors calculate the level of detection risk they must attain to achieve their desired audit risk. They then design evidence collection procedures in an attempt to achieve this level of detection risk.

In summary, the whole point to our considering the audit risk model is that audit efforts should be focused where they will have the highest payoffs. In most cases auditors cannot collect evidence to the extent they would like. Accordingly, they must be astute in terms of where they apply their audit procedures and how they interpret the evidence they collect. Throughout the audit they must continuously make decisions on what to do next. Their notions of materiality and audit risk guide them in making this decision.

Types of Audit Procedures:

When external auditors gather evidence to determine whether material losses have occurred or financial information has been materially misstated, they use five types of procedures:

1. **Procedures to obtain an understanding of controls:** Inquiries, inspections, and observations call be used to gain all understanding of what controls supposedly exist, how well they have been designed and whether they have been placed in operation.
2. **Tests of controls:** Inquiries, inspections, observations, and reperformance of control procedures can he used to evaluate whether controls are operating effectively.
3. **Substantive tests of details of transactions:** These tests are designed to detect dollar errors or irregularities in transactions that would affect the financial statements. For example, an external auditor might verify that purchase and disbursement transactions are correctly recorded in journals and ledgers.
4. **Substantive tests of details of account balances:** These tests focus on the ending general ledger balances in the balance sheet and income statement For example, an external auditor might circularize a sample of customers to test the existence and valuation of the debtors balance.
5. **Analytical review procedures:** These tests focus on relationships among data items with the objective of identifying areas that require further audit work. For example, an external auditor might examine the level of sales revenue across time to determine whether a material fluctuation that requires further investigation has occurred in the current year.

Steps in Information System Audit:

The Audit of an IS environment to evaluate the systems, practices and operations may include one or both of the following :

- Assessment of internal controls within the IS environment to assure validity, reliability, and security information.
- Assessment of the efficiency and effectiveness of the IS environment in economic terms.

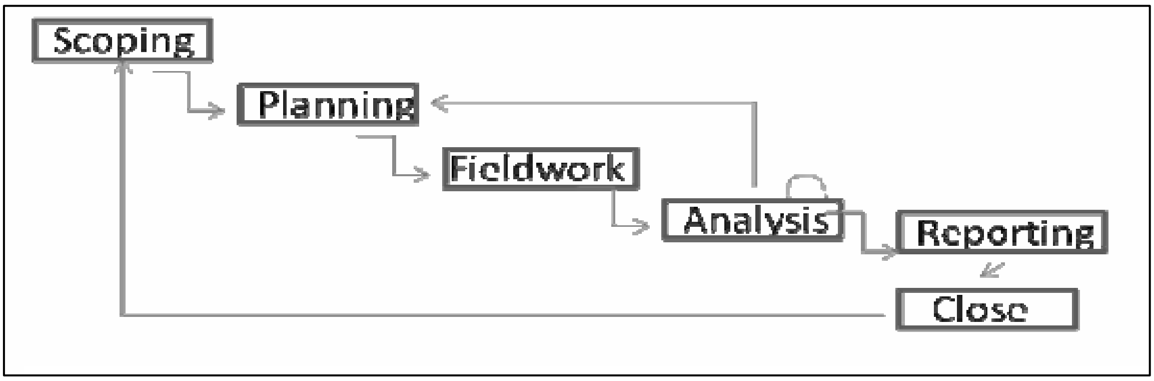
The IS audit process is to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole. This includes evaluating both the effectiveness and efficiency. The focus (scope and objective) of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness (result-orientation) and efficiency (optimum utilisation of resources)

Responsibility of IS Auditor:

The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor. The set of skills that is generally expected of an IS auditor include :

- ✓ Sound knowledge of business operations, practices and compliance requirements,
- ✓ Should possess the requisite professional technical qualification and certifications,
- ✓ An good understanding of information Risks and Controls,
- ✓ Knowledge of IT strategies, policy and procedure controls,
- ✓ Ability to understand technical and manual controls relating to business continuity, and
- ✓ Good knowledge of Professional Standards and Best practices of IT controls and security.

Steps in ISA: It can be categorized into six stages-



1) *Scoping and pre-audit survey* : the auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.
2) *Planning and preparation* : during which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.
3) *Fieldwork :* gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes etc.
4) *Analysis* : this step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Treats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.
5) *Reporting* : reporting to the management is done after analysis of data gathered and analysis.

6) *Closure* : closure involves preparing notes for future audits and following –up management to complete the actions they promised after previous audits.

Auditing Around or Through the Computer:

When auditors come to the controls testing phase of an information systems audit, one of the major decisions they must make is whether to test controls by auditing around or through the computer. The phrases **"auditing around the computer" and "auditing through the computer"** are carryovers from the past.

Today we recognize that the two approaches each have their merits and limitations and that each must be considered carefully in the context of planning and executing the most cost-effective audit. These approaches are –

- Evaluating computer systems simply by checking their input and output; known as "Auditing Around the Computer"
- Audits could not be conducted properly unless the internal workings of computer systems were examined and evaluated; known as "Auditing Through Computer"

Auditing Around the Computer:

Auditing around the computer involves arriving at an audit opinion through examining and evaluating management controls and then input and output only for application systems. Based on the quality of an application system's input and output, auditors infer the quality of the application system's processing. The application system's processing is not examined directly. Instead, auditors view the computer as a black box.

Auditors should audit around the computer when it is the most cost-effective way to undertake the audit. Auditing around the computer must be used in the following cases:

1) The system is simple and batch oriented.
2) Often it is cost-effective to audit around the computer when an application system uses a generalized package as its software platform.
3) If the package has been provided by a reputable vendor, has received widespread use, and appears error free, auditors might decide not to test the processing aspects of the system directly. Instead they might seek to ensure
    a. The organization has not modified the package in any way;
    b. Adequate controls exist over the source code, object code and documentation to prevent unauthorized modification of the package; and
    c. High-quality controls exist over input to and output from the package.
4) Auditors might audit around the computer when a high reliance is placed on user rather than computer controls to safeguard assets, maintain data integrity and attain effectiveness and

efficiency objectives.

Usually auditing around the computer is a simple approach to the conduct of the audit and it can be performed by auditors who have little technical knowledge of computers.

Limitations:

1) The type of computer system in which it is applicable is very restricted. It should not be used when systems are complex. Otherwise, auditors might fail to understand some aspect of a system that could have a significant effect on the audit approach.
2) It does not provide information about the system's ability to cope with change.

Auditing Through the Computer:

While auditing through the computer, the auditors use the computer to test (1) the processing logic and controls existing within the system and (2) the records produced by the system. Depending on the complexity of the application system, the task of auditing through the computer might be fairly simple or it might require extensive technical competence on the part of the auditor.

Auditing through the computer must be used in the following cases:

1. The inherent risk associated with the application system is high.
2. The application system processes large volumes of input and produces large volumes of output that make extensive, direct examination of the validity of input and output difficult to undertake.
3. Significant parts of the internal control system are embodied in the computer system, For example, in an online banking system, a computer program might batch transactions for individual tellers to provide control totals for reconciliation at the end of the day's processing.
4. The processing logic embedded within the application system is complex. Moreover, large portions of system code are intended to facilitate use of the system or efficient processing.
5. Because of cost-benefit considerations, substantial gaps in the visible audit trail are common in the system.

The primary advantage of auditing through the computer is that auditors have increased power to test an application system effectively. They can expand the range and capability of tests they can perform and thus increase their confidence in the reliability of the evidence collection and evaluation. Furthermore, by directly examining the processing logic embedded within an application system, auditors are better able to assess the system's ability to cope with change and the likelihood of losses or account misstatements arising in the future.

Disadvantages:

1) It can sometimes be costly, especially in terms of the labor hours that must be expended to understand the internal workings of an application system.
2) In some cases we will need extensive technical expertise, if we are to understand how the system works.

* * * * *