LITERATURE REVIEW (Chapter 2-5)
2.1 Introduction: -

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 rely on a sample of data to determine whether the objectives of information systems auditing are being achieved. In such a situation we perform information systems audits so that we obtain reasonable assurance that an organization safeguards its data-processing assets, maintains data integrity and achieves system effectiveness and efficiency.

2.2 The Nature of Controls: -

Information systems auditors ultimately are concerned with evaluating the feasibility 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. Unfortunately, we tend to name controls by focusing on just one feature of the control. For example, probably all of us are familiar with a password control. A password, per se, however, is not a control. Passwords become a control only in the context of a system that allows secure issue of or choice of passwords, correct validation of passwords, secure storage of passwords, follow-up on illicit use of passwords and so on. If this system breaks down in some way, passwords will be ineffective as a control. In short, the term "password control" is a notation for the constellation of things that work together to ensure only authorized people use computing resources. When we evaluate a control, therefore, we must consider its reliability from a system perspective.
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. Form 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. For example, a program could contain erroneous instructions that result in incorrect computations being performed. Whatever the reason, the system moves into a state that we deem to be unacceptable.

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.

2. **Detective control:** 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.

3. **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.

The overall purpose of controls is to reduce expected losses from unlawful events that can occur in a system. They do so in two ways. First, preventive controls reduce the probability of unlawful events occurring in the first place. For example, instructions on a source document reduce the likelihood of the clerk who completes the document
making an error. Second, detective and corrective controls reduce the amount of the losses that arise if the unlawful event occurs. For example, if a data-entry clerk keys incorrect data into a computer system, an input validation control might detect that the data is in error and halt further processing. A small loss arises from delayed processing, but larger losses associated with a corrupted database do not occur. In addition, the control might be able to determine the nature of the keying error made, perhaps on the basis of past keying errors and correct the error without the clerk having to intervene. Thus, the losses associated with recovering from the error are also reduced.

The auditor's task is to determine whether controls are in place and working to prevent the unlawful events that might occur within a system. Auditors must be concerned to see that at least one control exists to cover each unlawful event that might occur. Usually, some unlawful events in a system will not be covered because a cost-effective control cannot be found. Even if an unlawful event is covered by a control, however, auditors must evaluate whether the control is operating effectively. Moreover, if more than one control covers an unlawful event (i.e., redundant controls exist), auditors must ensure that all operate effectively. Otherwise, losses can be incurred because of reliance on a malfunctioning control instead of a reliable one.

2.3 Dealing with Complexity: -

Conducting an information systems audit is an exercise in dealing with complexity. Auditors somehow must accomplish their objectives given the myriad of systems. Because complexity is a root cause of the problems faced by many professionals, researchers have attempted to develop guidelines that reduce complexity. In the following subsections we consider two major guidelines that underlie the approach taken when conducting an information systems audit: -

1. Given the purposes of the information systems audit, factor the system to be evaluated into subsystems.

2. Determine the reliability of each subsystem and the implications of each subsystem's level of reliability for the overall level of reliability in the system.
The first step in understanding a complex system is breaking it up into subsystems. A subsystem is a component of a system that performs some basic function needed by the overall to enable it to attain its fundamental objectives. Subsystems are logical components rather than physical components. In other words, you cannot "touch" a subsystem. It exists only in the eye of the beholder. For example, we cannot see the input subsystem in a computer system. Instead, we see such things as terminals and data-entry clerks that function to get data into the system, but these things are components of the input subsystem and not the subsystem itself.

The process of decomposing a system into subsystems is called factoring. Factoring is an iterative process that terminates when we feel we have broken down the system into parts small enough to be understood and evaluated. In other words, each subsystem is decomposed into its constituent subsystems, which, in turn, are decomposed again until we can sufficiently comprehend the subsystem with which we are dealing. The system to be evaluated can then be described as a level structure of subsystems, with each subsystem performing a function needed by some higher-level subsystem.

To undertake the factoring process, we need some basis for identifying subsystems. The essence of a subsystem is the function it performs. Auditors should look first; therefore, for the fundamental functions a system performs to accomplish its overall objectives. Different functions delineate different subsystems. Besides function, systems theory indicates that two other guidelines should underlie the way in which we identify and delineate subsystems. First, each subsystem should be relatively independent of other subsystems. The objective is for each subsystem to be loosely coupled to other subsystem. If this objective can be achieved, auditors can evaluate the subsystem in relative isolation from other subsystems. In other words, to some extent auditors can disregard the effects of control strengths and weaknesses in other systems. Second, each subsystem should be internally cohesive. All the activities performed by the subsystem should be directed toward accomplishing a single
function. If this objective can be achieved, it will be easier for auditors to understand and evaluate the activities carried out by the subsystem.

At least conceptually, auditors might choose to factor systems in several different ways. Over time, however, auditors have found two ways to be especially useful when conducting information systems audits. The first is according to the *managerial functions* that must be performed to ensure that development, implementation, operation and maintenance of information systems proceed in a planned and controlled manner. Managerial systems function to provide a stable infrastructure in which information systems can be built, operated and maintained on a day-to-day basis. Several types of management subsystems have been identified that correspond to the organizational hierarchy and some of the major tasks performed by the information systems function: -

<table>
<thead>
<tr>
<th>Management Subsystem</th>
<th>Description of Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top management</td>
<td>Top management must ensure the information system function is well managed. It is responsible primarily for long-run policy decisions, on how information systems will be used in the organization.</td>
</tr>
<tr>
<td>IS management</td>
<td>Information systems management has overall responsibility for the planning and control, of all information systems activities. It also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.</td>
</tr>
<tr>
<td>Systems development Management</td>
<td>Systems development management is responsible for the design, implementation and maintenance, of application systems.</td>
</tr>
</tbody>
</table>
Management Programming management is responsible for programming new systems, maintaining old systems and providing general systems support software.

Data administration Data administration is responsible for addressing planning and control issues in relation to use, of an organization's data.

Quality assurance Management Quality assurance management is responsible for ensuring information systems development, implementation, operation and maintenance conform to established quality standards.

Security administration Security administration is responsible for access controls and physical security, over the information systems function.

Operations management Operations management is responsible for planning and control, of the day-to-day operations, of information systems.

The second factoring is according to the application functions that need to be undertaken to accomplish reliable information processing. This factoring corresponds to the "cycles" approach auditors have traditionally used to conduct an audit. The information systems supporting an organization are first grouped into cycles. These cycles vary across industries, but a typical set for a commercial or manufacturing enterprise includes (a) sales and collections, (b) payroll and personnel, (c) acquisitions and payments (d) conversion, inventory and warehousing and (e) treasury. Each cycle is then factored into one or more application systems. For example, the sales and collections cycle comprises an order-entry application system, a billing application
Application systems, in turn, are then factored into subsystems. The set of application subsystems includes the following:

<table>
<thead>
<tr>
<th>Application Subsystem</th>
<th>Description of Subsystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boundary</td>
<td>Comprises the components that establish the interface between the user and the system. Input comprises the components that capture, prepare and enter commands and data into the system.</td>
</tr>
<tr>
<td>Communication</td>
<td>Comprises the components that transmit data among subsystems and systems.</td>
</tr>
<tr>
<td>Processing</td>
<td>Comprises the components that perform decision making, computation, classification, ordering and summarization of data in the system.</td>
</tr>
<tr>
<td>Database</td>
<td>Comprises the components that define, add, access, modify, and delete data in the system.</td>
</tr>
<tr>
<td>Output</td>
<td>Comprises the components that retrieve and present data to users of the system.</td>
</tr>
</tbody>
</table>

Neither of these two types of decomposition is irrevocable, and in due course others might prove better. Nevertheless, they currently underlie the audit approaches advocated by many professional bodies of auditors. They allow decreasing complexity to a point where one can understand and evaluate the nature of and reliability of subsystems.
2.3.2 Assessing Subsystem Reliability:

After the identification of the lowest-level subsystems in level structure of subsystems, one may evaluate the reliability of control. Beginning with the lowest-level subsystems, we first attempt to identify all the different types of events that might occur in these subsystems. We must be mindful of both the lawful events and the unlawful events that can occur. Nevertheless, an auditor's primary concern will be with any unlawful events that might arise.

As a basis for identifying lawful and unlawful events in management subsystems, we focus on the major functions each subsystem performs. We consider how each function should be undertaken and then evaluate how well a subsystem complies with our normative views. For example, an important function that should be performed by the top-management subsystem is information systems planning. Given the nature of the organization we are auditing, we might determine that top management should undertake extensive strategic planning but only a moderate level of operational planning if the long-run future of information systems within the organization is to be ensured. These views form the basis for determining which information systems planning events are to be deemed lawful and which are to be deemed unlawful. We then identify the information systems planning events that have occurred and classify them as either lawful or unlawful. For example, if no strategic planning has been undertaken, an unlawful event has occurred. Failure to plan ultimately undermines asset safeguarding, data integrity, system effectiveness, and system efficiency objectives. Similarly, if too much operational planning has been undertaken, an unlawful event has occurred because resources have been wasted. As a result, system effectiveness and system efficiency objectives have been undermined.

Perhaps the key aspect of identifying lawful and unlawful events in management subsystems is the decision of how a particular function should be performed within the subsystem. After substantial research on information systems management, it is now clear that the way information systems management, functions should be performed in organizations must vary, depending on the particular circumstances faced by each organization. For example, in some organizations, strategic information
systems planning are a critical function, but in others it has only minor importance. Auditors must be knowledgeable and astute in determining the ways that management functions should be performed in each organization evaluated. Otherwise, judgments on what events are lawful will be misguided.

As a basis for identifying lawful and unlawful events in application subsystems, we focus on the transactions that can occur as input to the subsystem. All events in an application system must arise from a transaction. The application system initially changes state (an event occurs) when the transaction is first received as an input. For example, an order-entry system must record an order when it is first entered into the system. Further state changes (events) then occur as the application system processes the transaction. For example, after an order-entry system has stored an open order, it then attempts to fill the order. Lawful events will arise if the transaction and subsequent processing are authorized, accurate, complete, non-redundant, effective and efficient. Otherwise, unlawful events will occur.

To identify all the events that might arise in an application system as a result of a transaction, we must understand how the system is likely to process the transaction. Historically, auditors have used walk-through techniques to accomplish this objective: They consider a particular transaction, identify the particular components in the system that process the transaction and then try to understand each processing step that each component executes. They also consider any errors or irregularities (unlawful events) that might occur along the way. For example, auditors might focus on a credit-sale transaction. After the transaction has been entered into the sales system, they would trace the credit sale through each processing step executed by the order-entry program. They would also consider how the transaction might be entered improperly and how subsequent processing errors or irregularities might arise.

It is often costly to trace each individual transaction through an application system to obtain an understanding of all the different types of events that can occur in the system. For this reason, auditors sometimes focus on classes of transactions. In other words, they group transactions together if the transactions undergo similar processing.
They then try to understand these transactions and the events that arise as a result of these transactions as a group. In addition, they focus only on those transactions they consider to be material from the viewpoint of their audit objectives. Using these strategies, not all events that can occur in a system are identified. Nevertheless, auditors should examine all those transactions and events that they consider to be important.

When the material events that can occur in a management of application system have been identified, auditors must evaluate whether controls are in place and working to cover the unlawful events. Accordingly, they collect evidence on the existence and reliability of controls to determine whether expected losses from unlawful events have been reduced to an acceptable level. They consider each type of unlawful event that might arise, whether controls cover each of these events, how reliable these controls are and whether a material error or irregularity can still occur. Lists have been published to assist with this task, showing failings that occur in management subsystems and errors and irregularities that occur for different types of transactions in different types of application systems. These lists also show various controls that can be used to reduce expected losses from these errors and irregularities.

The evaluation of reliability proceeds upwards in the level structure of a system. Lower-level subsystems are components of higher-level systems. When the reliability of a lower-level system has been assessed, its impact on the nature of and frequency of unlawful events in higher-level systems can be evaluated. The evaluation proceeds until the highest-level system (the entire system) has been considered. For every system at every level in the level structure, the evaluation steps are the same. The transactions that might enter the system are first identified. The lawful and unlawful events that can occur as a result are then considered. Finally, the reliability of the controls that cover the unlawful events is assessed.

As we evaluate higher-level systems, we are likely to encounter new controls for three reasons. First, controls in lower-level systems can malfunction. Recall, a control is a system itself and it can be unreliable like any other system. A higher-level control
might be implemented to cover unlawful events that arise when lower-level controls fail to prevent, detect or correct them. For example, consider a group of clerks that process mail orders. Work might be divided among them based on the first letter of customers' surnames. Thus, several subsystems exist to process orders from different groups of customers. Each clerk might exercise certain controls to prevent, detect or correct errors. Nevertheless, their manager might also examine the quality of their work. Managers are responsible for the quality of work in all subsystems and they are exercising a higher-level control in case a lower-level control malfunctions.

Second, it might be more cost-effective to implement controls at higher levels. Again, consider our example of the group of clerks who process mail orders. If they are well trained and diligent, they might not be required to double-check their work. Given the low error rate that is expected to occur, the cost of double checking might be too high. Their manager periodically might take a sample of their work, however, to assess its quality. The higher-level control is more cost-effective because it is exercised by one person who has greater facility with control.

Third, some events are not manifested as unlawful except in higher-level systems. For example, an employee might query a database to obtain the average salary of female consultants employed within an organization. The subsystem that processes the query might deem this query to be a lawful event. The person might then query the database to obtain the number of female consultants employed within the organization. Again, the subsystem that processes the query might deem it to be lawful. If the organization employs only one female consultant, however, the employee now knows the consultant's salary. A higher-level system control is needed to detect the violation of the confidentiality of her salary. When the two lawful events are considered together, the overall event is unlawful.

Clearly, the process of aggregating subsystem reliability assessments to higher levels can be a difficult task. Errors made at one level of assessment will propagate to higher levels of assessment. Auditors must take substantial care with evidence-collection processes and evaluation judgments, especially as they begin to fix evaluation
judgments in lower-level subsystems and move to higher-level subsystems and systems.

2.4 **Audit Risks:**

The auditors are concerned with four objectives: asset safeguarding, data integrity, system effectiveness and systems 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. Internal auditors may 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.

Further the 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 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?) and accounting and auditing concerns (e.g., Are creative accounting practices used?). Auditors then consider the inherent risk associated with different segments of the audit (cycles, application systems and financial statement accounts). For each segment, auditors consider the following factors.
**Inherent Risk Factor** | **Explanation**
--- | ---
Financial system | Those systems that usually provide financial control over the major assets of an organization—e.g., cash receipts and disbursements, payroll, accounts receivable and payable often have higher inherent risk. They are frequently the target of fraud and embezzlement.

Strategic system | Those systems that provide an organization with a competitive advantage—e.g., systems that lock in customers or suppliers or embody a patent or trade secret—often have high inherent risk. They might be the target of industrial espionage or retaliatory actions by a competitor.

Critical operational | Those systems that could cripple an organization if they fail—e.g., customer reservations systems or production control systems—often have high inherent risk.

Technologically advanced Systems | Those systems that use advanced technology often have high inherent risk because they are complex and the organization lacks experience with them.

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 usually identify and evaluate controls in management subsystems first. Management (subsystem) controls are fundamental controls because they cover all application systems. Thus, the absence of a management control is a serious concern for auditors. Conceptually, 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. In addition, it is often more efficient if auditors evaluate management controls before application controls. After auditors have evaluated a management control, auditors usually do not have to evaluate it again because it should function across all applications. For example, if auditors find that an organization enforces high-quality documentation standards, it is unlikely they will have to review the quality of documentation for each application system.

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. To estimate the level of detection risk they might achieve with a set of audit procedures, they must have a good understanding of how likely these audit procedures are to detect a material loss or account misstatement when one exists. Moreover, auditors must evaluate how reliably the audit procedures are likely to be applied. Not only must they choose audit procedures that have the capacity to provide us with a desired level of detection risk, they also must ensure they are properly executed.

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 continually make decisions on what to do next. Their notions of materiality and audit risk guide them in making this decision.

2.5 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:
Procedures to obtain an understanding of controls: Inquiries, inspections and observations can be used to gain an understanding of what controls supposedly exist, how well they have been designed and whether they have been placed in operation.

Tests of controls: Inquiries, inspections, observations and re-performance of control procedures can be used to evaluate whether controls are operating effectively.

Substantive test 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.

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.

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.

Auditors can use similar types of procedures if they are concerned with evaluating the effectiveness and efficiency of an organization's operations:

1. Procedures to obtain an understanding of controls: Inquiries, inspections and observations can be used to gain an understanding of the administrative controls set up to achieve effectiveness and efficiency objectives rather than the accounting controls set up to achieve asset safeguarding and data integrity objectives.

2. Tests of controls: Tests of controls focus on whether administrative controls have been well designed and whether they are operating effectively. For example, auditors might interview an operations manager to check whether she/he regularly reviews the response-time performance of a critical online...
system and if so, what action she/he takes when response times are unacceptable.

3. **Substantive tests of details of transactions:** From an effectiveness and efficiency perspective, auditors still have a notion of substantive tests of details of transactions. Using the response-time example discussed previously, auditors might check the response times for a sample of individual transactions to determine whether they are within acceptable bounds.

4. **Substantive tests of overall results:** The notion of account balances does not apply in the context of effectiveness and efficiency concerns. Nevertheless, auditors have a notion of overall effectiveness and efficiency results. For example, management might assert the average response time for an application system over a 12-month period is two seconds. As a substantive test of this claimed overall result, auditors might survey users of the system to determine its validity.

5. **Analytical review procedures:** Analytical review procedures are still relevant in the context of effectiveness and efficiency concerns. For example, auditors might build a queuing model or a simulation model of an application system to evaluate whether the resources consumed by the application system seem reasonable.

Often, the order of test from the least costly to the most costly is as follows: - analytical review procedures, procedures to obtain an understanding of controls, test of controls, substantive test of details of transactions and substantive test of balances/overall results. On the other hand, the other is reversed when we consider the reliability and information content of the evidence provided by the different audit procedures. Accordingly, auditors usually carry out the less costly audit procedures first in the hope the evidence obtained from these procedures indicates it is unlikely a material loss or material misstatement has occurred or will occur. If this outcome arises, auditors can alter the nature, timing, and extent of the more costly tests used. For example, on the basis of their understanding of controls and tests of controls, auditors might conclude controls are well designed and operating effectively. In this light, they would seek to reduce the costs of substantive testing in the following ways:
change the nature of substantive testing by employing less costly substantive test
directed toward internal parties rather than external parties; change the timing of
substantive testing by spreading it across a longer period to reduce costs and change
the extent of substantive tests by choosing smaller sample sizes to reduce costs.

2.6 **Overview of Steps in an Audit:**

Keeping in mind the lessons in the previous sections on the nature of controls, the
importance of system factoring in reducing complexity, the nature and consequences
of audit risks and the types of audit procedures auditors can carry out. The following
subsections briefly describe each step in an audit and highlight those parts of the audit
where the information systems auditor often plays an important role. Though imply a
sequential progression of audit steps, some steps can be carried out concurrently and
some iteration of steps can occur. For example, some tests of controls could be carried
out as auditors attempt to understand the controls that are supposed to be in place.
Furthermore, while both external and internal auditors will follow the general
approach, the decisions they take at each step in the audit might vary because they
have different roles. For example; internal auditors might spend more time testing
controls because they are more concerned than external auditors about the efficiency
of the controls. The following discussion points out how external and internal auditors
might differ in the decisions they take at each stage of the audit.

2.6.1 **Planning the Audit:**

Planning is the first phase of an audit. For an external auditor, this means
investigating new and continuing clients to determine whether the audit engagement
should be accepted, assigning appropriate staff to the audit, obtaining an engagement
letter, obtaining background information on the client, understanding the client's legal
obligations and undertaking analytical review procedures to understand the client's
business better and identify areas of risk in the audit. For an internal auditor, this
means understanding the objectives to be accomplished in the audit, obtaining
background information, assigning appropriate staff and identifying areas of risk.
During the planning phase, auditors must decide on the preliminary materiality level to be set for the audit, an external auditor's concern will be the size of misstatements in the financial statements that would affect the decisions of users of the financial statements. Internal auditors might also be concerned about the size of losses that have arisen or might arise through ineffective or inefficient operations.

Auditors must also make a judgment on desired audit risk. Usually the level of desired audit risk is set for the overall audit rather than for segments of it. For external auditors, this reflects the risk they are willing to take to issue an unqualified opinion even though the financial statements are materially in error. For internal auditors, desired audit risk might also reflect the risk they are willing to take to issue an unqualified opinion even though material losses have occurred or might occur through ineffective or inefficient operations.

The levels of inherent risk will vary across different segments of the audit. Some segments are more susceptible to errors, irregularities, ineffectiveness, and inefficiencies. Auditors must consider each segment of the audit in turn and evaluate the factors that lead to inherent risk associated with the segment. For example, systems that involve handling of cash are susceptible to defalcations; technologically complex systems are susceptible to inefficient use of resources.

Perhaps the most difficult decision to make in the planning phase is the judgment on the level of control risk associated with each segment of the audit. When making this judgment, information systems audit skills are especially important. The American Institute of Certified Public Accountants (1995) argues that to decide on the level of control risk, auditors must first understand the internal controls used within an organization. Internal controls comprise five interrelated components:

- **Control environment:** Elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's philosophy and operating style, the ways authority and
responsibility are assigned, the way the audit committee functions, the methods used to plan and monitor performance, and so on.

*Risk assessment:* Elements that identify and analyze the risks faced by an organization and the ways these risks can be managed.

*Control activities:* Elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded and independent checks on performance and valuation of recorded amounts occur. These elements are usually called accounting controls. Internal auditors, however, also might be concerned with administrative controls established to achieve effectiveness and efficiency objectives.

*Information and communication:* Elements in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities properly.

*Monitoring:* Elements that ensure internal controls operate reliably over time.

In the context of the concepts examined earlier in this chapter and the role information systems auditors perform, understanding internal controls in an organization involves factoring and examining both management controls and application system controls. Auditors can understand the control environment and risk assessment components primarily by examining management controls. For example, when auditors determine whether an information systems steering committee exists, they seek to understand the control environment and risk assessment components of internal control. Auditors can understand specific control activities by reviewing both management controls and application controls. For example, when auditors review those activities associated with production release of programs or entry of data to an application system, they are seeking to understand the control activities undertaken.

Auditors can understand the information and communication component by examining both management controls and application controls. For example, when auditors examine how management communicates roles and responsibilities or how transactions are captured, recorded, processed and summarized within an application...
system, they are seeking to understand the information and management component. Auditors can understand the monitoring component primarily by examining management controls. For example, when auditors examine the ways management evaluates employee performance, they are seeking to understand the monitoring component.

Management controls can differ substantially from organization to organization. For example, an organization might have all information processing performed at a single site that is under the control of a single information systems department. In this situation, there is only one management system to evaluate—that associated with the information systems department. Auditors would factor this system into various subsystems—top management systems development management, programming management and so on—and seek to understand internal controls in the context of each of these subsystems.

On the other hand, another organization's information systems function might be widely dispersed. For example, the organization might have a highly decentralized structure. Divisions might have responsibility for developing, operating and maintaining their own information systems. Each might have its own computer center and information systems staff. End-user computing also could be substantial. Some end users might be developing, maintaining and operating their own systems. In these circumstances, auditors must evaluate multiple management systems: one for each divisional site and perhaps one for each major end-user computing site. They must consider each management system in turn, evaluate the risks associated with each and factor those that are material into their various subsystems. In short, auditors might have to examine multiple top-management subsystems, multiple systems development management subsystems, multiple programming management subsystems and so on, to understand the internal controls.

Application controls also might be substantially diverse. In a highly centralized organization, there might be only one set of cycles to evaluate. In a highly decentralized organization, however, there might be multiple sets of cycles, each of
which must be evaluated. For example, each division might have its own sales and collections cycle, payroll and personnel cycle, acquisitions and payments must identify those cycles that are material to the audit, factor the cycles into application systems and subsystems, understand these systems and subsystems and identify the controls that have been implemented over each important class of transactions that passes through the different systems and subsystems.

There are several types of evidence collection techniques used to understand the internal controls: - review of working papers from prior audits, interviews with top management and information systems personnel, observations of activities carried out within the information systems function and reviews of information systems documentation. The evidence can be documented by completing questionnaires, constructing high-level flowcharts and decision tables and preparing narratives. A computer can be helpful to employ these techniques and auditors might use a computer-aided software engineering (CASE) tool to draw flowcharts. Similarly, they might interact with questionnaire software that elicits responses on the status of various types of internal controls. Auditors must be careful not to undertake too much work, however, during this phase. The goal is to obtain just enough information to understand internal controls and to decide how to proceed with the audit.

After obtaining a satisfactory understanding of the internal controls, auditors must assess the level of control risk. External auditors assess control risk in terms of each major assertion that management should be prepared to make about material items in the financial statements. Thus auditors must relate their understanding of internal controls to the impact they ultimately have on the figures presented in the financial statements. In the case of management controls, the relationship usually is indirect and if careful control is exercised over program maintenance, auditors might have increased confidence that a specific control in an application system will continue to be exercised properly throughout the financial period. As a result, they would be confident the control supports, say, the completeness assertion for a particular financial statement component. In the case of application controls, the relationship to financial statement components is usually fairly direct. If the control has not been
designed properly or has not been operated effectively, the potential impact on a financial statement assertion is usually clear.

Internal auditors can also assess control risk in terms of assertions that management implicitly or explicitly make about the effectiveness and efficiency of systems. For example, management might say a system achieves a certain throughput rate and that customers of the organization who use the output of the system have a certain level of satisfaction with the performance of the system. Auditors must use their understanding of the internal controls to evaluate whether they have been designed appropriately and whether they have been placed in operation to support management's assertions.

After auditors obtain an understanding of the internal controls, they then must determine the control risk in relation to each assertion:

If auditors assess control risk at less than the maximum level, they must then identify the material controls that relate to the assertion and test the controls to evaluate whether they are operating effectively. They work on the assumption that tests will show that if the controls are operating effectively they can reduce the extent of substantive testing needed to reach an audit opinion.

If auditors assess control risk at the maximum level, they do not test controls; they might conclude that internal controls are unlikely to be effective and therefore cannot be relied upon or that a more effective and efficient audit can be conducted using a substantive approach.

2.6.2 Tests of Controls:

Auditors, test controls when they assess the control risk for an assertion at less than the maximum level. They rely on controls as a basis for reducing more costly testing. At this stage in the audit, however, auditors do not know whether the controls
identified operate effectively. Tests of controls, therefore, evaluate whether specific, material controls are, in fact, reliable.

This phase usually begins by again focusing first on management controls. If testing shows that, contrary to expectations, management controls are not operating reliably, there might be little point to testing application controls. If auditors identify serious management-control weaknesses, they might have to issue an adverse opinion or undertake substantive tests of transactions and balances or overall results. Auditors conduct the evaluation iteratively for each management subsystem and each application subsystem that is material to the assertion. If auditors conclude that management controls are in place and working satisfactorily, they then would evaluate the reliability of application controls by tracing instances of material classes of transactions through each significant control exercised in the various application subsystems. For each transaction considered, auditors evaluate whether the control is operating effectively.

After auditors have completed tests of controls, they again assess control risk. In light of the test results, they might revise the preliminary assessment of control risk downwards or upwards. In other words, auditors might conclude that internal controls are stronger or weaker than initially anticipated. They might also conclude that it is worthwhile to perform more tests of controls with a view to further reducing the substantive testing. Perhaps internal controls are stronger than initially believed. Accordingly, auditors conclude control risk has decreased and seek further evidence to support this assessment.

During the controls testing phase, internal auditors and external auditors might differ in their approaches to the audit. If internal auditors identify control weaknesses, they might expand their investigations to gain a better understanding of the nature of and implications of these weaknesses. Their objective might be to provide in-depth recommendations to rectify the control weaknesses. External auditors, on the other hand, will tend to cut short their investigations when they identify control weaknesses
and proceed to undertake expanded substantive tests in light of the increased control risk they perceive.

2.6.3 **Tests of Transactions:**

Typical attest tests of transactions include tracing journal entries to their source documents, examining price files for propriety and testing computational accuracy. The computer is quite useful to perform these tests, and auditors might use generalized audit software to check whether the interest paid on bank accounts has been calculated correctly. From an operational perspective, auditors use tests of transactions to evaluate whether transactions or events have been handled effectively and efficiently. For example, to indicate a database system's effectiveness, auditors might examine a sample of queries recorded on a transaction log to evaluate whether the queries have been generated by a wide cross-section of users of the database system. To evaluate efficiency, auditors might examine the turnaround times for a sample of jobs submitted to an application system. Again, the computer can help to carry out these tests. For example, auditors may use generalized audit software to select a sample of database queries from a transaction log for evaluation.

In an attest audit, auditors conduct tests of transactions at interim dates in order to reduce the amount of substantive tests of balances to be done at financial year end and thus to reduce the overall costs of the audit. In an operational audit for effectiveness and efficiency purposes, auditors also use tests of transactions at interim dates in order to reduce the amount of substantive testing of overall results to be done near the reporting date. For example, if the response times for a sample of transactions that occur throughout the period under review are satisfactory, auditors can reduce the number of users surveyed near the report date to determine whether they consider response times to be satisfactory. To follow this strategy, auditors must know an operational audit is required well in advance of the reporting date.

If the results of tests of transactions indicate that material losses have occurred or might occur or that financial information is or might be materially misstated, substantive tests of balances or overall results will be expanded. Auditors can use
expanded tests of balances or overall results to obtain a better estimate of the losses or misstatements that have occurred or might occur.

2.6.4 Tests of Balances or Overall Results:

Auditors conduct tests of balances or overall results to obtain sufficient evidence for making a final judgment on the extent of losses or account misstatements that occur when the information systems function fails to safeguard assets, maintain data integrity and achieve system effectiveness and efficiency. In general, tests of balances or overall results are the most expensive of the audit (although Clowes 1988 argues that the costs and benefits of the different types of tests conducted during different phases is changing as the tests become increasingly automated). Thus, auditors should design and execute these tests carefully.

To understand the approach in this phase, consider, first, the asset-safe-guarding and data-integrity objectives. Some typical substantive tests of balances used are confirmation of receivables, physical counts of inventory and recalculation of depreciation on fixed assets. Recall that if auditors believe controls are reliable on the basis of prior audit work, they will limit the number and scope of these tests because material losses or material account misstatements that have arisen through failure to safeguard assets and maintain data integrity are not expected. On the other hand, if auditors believe controls are no reliable, they will need to expand the extent of substantive tests of balances to estimate better the size of the losses and account misstatements.

Consider, now, the system-effectiveness and system-efficiency objectives. The tests conducted to estimate losses from failure to achieve these objectives are less clear cut than those associated with asset safeguarding and data integrity objectives. For example, auditors might work with users of an application system to estimate the losses they believe have arisen because the system does not provide them with the output they require to make high-quality decisions. As another example, auditors might attempt to estimate the costs of inefficiencies that have occurred because failures in information systems planning have resulted in inappropriate hardware
purchases. Again, the extent of the audit work performed depends on the auditor's prior assessment of the reliability of administrative controls.

As with the prior phases, the nature and conduct of the audit work during this phase can vary considerably, depending on the type of organization auditors are examining. At one extreme the audit could be a small organization that has a single, centralized information systems function. The audit work focuses on, the losses and account misstatements that might have arisen from a limited number of sources. At the other extreme, the audit could be of a large, decentralized organization in which the information systems function is widely dispersed. The audit work must be extensive to take into account losses and misstatements that could have arisen from a large number of sources.

2.6.5 Completion of the Audit:

In the final phase of the audit, auditors undertake several additional tests to bring the collection of evidence to a close. For example, they undertake reviews for subsequent events (events that occur subsequent to the financial statement date but that affect the information that should be reported in the financial statements) and contingent liabilities (potential liabilities that must be disclosed in the financial statement). They must then formulate an opinion about whether material losses or account misstatements have occurred and issue a report. The professional standards in many countries require one of four types of opinion be issued:

1. Disclaimer of opinion: On the basis of the audit work conducted, the auditor is unable to reach an opinion.

2. Adverse opinion: The auditor concludes that material losses have occurred or that the financial statements are materially misstated.
3. **Qualified opinion**: The auditor concludes that losses have occurred or that the financial statements are misstated but that the amounts are not material.

4. **Unqualified opinion**: The auditor believes that no material losses or account misstatements have occurred.

In addition to asset safeguarding and data integrity concerns, internal auditors might also have to decide whether material losses have occurred because the information systems function has failed to achieve system effectiveness and efficiency objectives. Unlike the asset safeguarding and data integrity objectives, the form of the audit opinion relating to system effectiveness and efficiency objectives is not prescribed by professional standards. Therefore, auditors must formulate their wording for the opinion so that it clearly communicates the findings and judgment. Nevertheless, a typical report would include an introduction that describes the audit objectives, scope, and general approach employed, a summary of critical findings, recommendations to address the major issues that arise from the findings, and data to support the critical findings listed in the report.

Auditors are also concerned with prognoses about losses and account misstatements. In other words, even though auditors might have concluded no material losses or misstatements have occurred, they might believe control weaknesses exist that mean such losses or misstatements could occur in the future. These weaknesses might motivate a concern about the viability of the organization if a major threat eventuates. In addition, auditors might be concerned about contingent liabilities associated with losses that arise through significant control weaknesses. For example, customers could sue an organization if it cannot provide products or services because its computer systems are not operational. At the conclusion of an audit, therefore, an important function that auditors perform is to provide management with a report documenting any control weaknesses they have identified, the potential consequences of these control weaknesses and some recommendation for remedial actions.
References: -


5. www.acl.com

6. www.cit.icai.org

7. www.icai.org

8. www.idea.com

9. www.isaca.org