**Conducting an Information Systems Audit**

**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 per· form 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.

How, then, can we perform information systems audit so that we obtain reasonable assurance that an organization safeguards its data-processing assets, maintains data integrity, and achieves system effectiveness and efficiency?

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.

We then consider the basic steps to be undertaken in the conduct of an information systems audit. 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:**

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.
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 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.

**Dealing with Complexity:**

Conducting an information systems audit is an exercise in dealing with complexity. Because complexity is a root cause of the problems faced by many professionals (e.g. engineers, architects), researchers have attempted to develop guidelines that reduce complexity. In the following subsections we consider two major guide lines 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.

**Subsystem Factoring:**

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 system 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, hut these things are components of the input subsystem and not the subsystem itself.

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

An understanding of complex systems can only be obtained if each of their parts can be studied relatively independently and the activities performed by each part are clear. When we decompose a system into subsystems, therefore, we should evaluate the extent of coupling and cohesion in the subsystems we choose. If the subsystems are not loosely coupled and internally cohesive, we should attempt a different factoring. If no factoring seems to delineate subsystems that possess these characteristics, we will have difficulty evaluating the reliability of the system because its activities are too convoluted. Indeed, auditors have long recognized that some systems cannot be audited. The theory of coupling and cohesion provides the underlying rationale for this conclusion when such systems are encountered.

**Assessing Subsystem Reliability:**

After we have identified the lowest-level sub-systems in our level structure of subsystems, we can evaluate the reliability of controls. Beginning with the lowest-level subsystems, we first attempt to identify all the different types of events that might occur in these sub-systems. We must be mindful of both the lawful events and the unlawful events that can occur.

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.

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.

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.

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.

**Steps in Information System Audit:**

1. **Establish the Terms of the Engagement:**

This will allow the auditor to set the scope and objectives of the relationship between the auditor and the organization. The engagement letter should address the responsibility (scope, independence, deliverables), authority (right of access to information), and accountability (auditee rights, agreed completion date) of the auditor.

1. **Preliminary Review:**

This phase of the audit allows the auditor to gather organizational information as a basis for creating their audit plan. The preliminary review will identify an organization’s strategy and responsibilities for managing and controlling computer applications. An auditor can provide an in depth overview of an organization’s accounting system to establish which applications are financially significant at this phase. Obtaining general data about the company, identifying financial application areas, and preparing an audit plan can achieve this.

1. **Obtain understanding of control structure:**

Understanding control structure in an organization involves examining both management controls and application controls. An internal control system should be designed and operated to provide reasonable assurance that an organization’s objectives are being achieved in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

To develop their understanding of internal controls, the auditor should consider information from previous audits, the assessment of inherent risk, judgments about materiality, and the complexity of the organization’s operations and systems.

Once the auditor develops their understanding of an organization’s internal controls, they will be able to assess the level of their control risk (the risk a material weakness will not be prevented or detected by internal controls).

1. **Assess control risk:**

After obtaining satisfactory understanding of internal controls, auditor must assess the level of control risk. Auditors assess control risk in terms of each major assertion that management should be prepared to make about material items in financial statements

|  |  |
| --- | --- |
| Existence | Assets, liabilities included in financial statements actually exist |
| Occurrence | All transactions represent events that have actually occurred |
| Completeness | All transitions have been recorded and presented |
| Rights and obligations | Assets are rights and liabilities are obligations of the organization at balance sheet date |
| Valuation or allocation  | Asset, liabilities, equity, reserves are been recorded at correct amount |
| Presentation and disclosure | All items of financial statements have been properly classified described and disclosed |

 After auditors obtain understanding of internal controls they must determine control risk in relation to each assertion.

1. If auditors assess controls at less than maximum level, they go to next step and test the controls to evaluate whether they are operating effectively.
2. If auditors assess control risk at higher than maximum level, they will not test controls at all, and carry out detailed substantive check procedures.
3. **Test of controls:**

In this step the auditors will test controls to ascertain whether they are operating effectively or not. Auditors will carry out testing of both application and management controls. This phase usually begins by focusing on management controls. If testing shows that control to expectations, management controls are not operating reliably, there may be little point in testing application controls, in such case auditors may qualify their opinion or carry out substantive tests in detail.

1. **Reassess controls:**

After auditors have completed tests of controls, they again assess the control risk. In light of test results, they might revise the anticipated control risk upward or downward. In other words auditor may conclude that internal controls are stronger or weaker than anticipated. They may also conclude that it is worthwhile to perform more tests to further reduce substantive testing.

1. **Completion of audit:**

In the final phase of audit, Audit procedures are developed based on the auditor understands of the organization and its environment. A substantive audit approach is used when auditing an organization’s information system. Once audit procedures have been performed and results have been evaluated, the auditor will issue either an unqualified or qualified audit report based on their findings.

**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 Josses 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 det6rmine 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, bow 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 rests 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.

**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. They arose during the period when auditors were debating how much technical knowledge was required to audit computer systems. Some argued that little knowledge was needed because auditors could evaluate computer systems simply by checking their input and output. Others contended audits could not be conducted properly unless the internal workings of computer systems were examined and evaluated. Unfortunately, the arguments of the former group were sometimes motivated by their lack of technical knowledge about computers. 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.

**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. This circumstance often arises when an application system has three characteristics.

**First,** the system is simple and batch oriented.

**Second,** often it is cost-effective to audit around the computer when an application system uses a generalized package as its software platform. 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 (1) the organization has not modified the package in any way; (2) adequate controls exist over the source code, object code and documentation to prevent unauthorized modification of the package; and (3) high-quality controls exist over input to and output from the package.

**Third,** 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. In testing, the focus is on the reliability of user controls rather than the reliability of computer controls.

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. The audit should be managed, however, by someone who has expertise in information systems auditing.

The approach has **two major limitations**. **First,** 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. **Second,** it does not provide information about the system's ability to cope with change. Systems can be designed and programs can be written in certain ways to inhibit their degradation when user requirements 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.

The approach has **two disadvantages**. **First,** 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. **Second**, in some cases we will need extensive technical expertise, if we are to understand how the system works.