CHAPTER 17

INFORMATION SYSTEM AUDITING AND ASSURANCE

As more and more accounting and business systems were automated, it became more and more evident that the field of auditing had to change. As the systems being audited increased their use of technology, new techniques for evaluating them were required. This chapter focuses on computer or ***information systems (IS) auditing***. It begins with a discussion of how the auditing profession has expanded in response to the spread of technology.

The objectives of this chapter are:

- to understand the general purpose of an audit and to have a firm grasp of the basic conceptual elements of the audit process;
- to know the difference between internal and external auditing and to be able to explain the relationship between these two types of auditing;
- to understand how auditing objectives and tests of control are determined by the control structure of the firm that is being audited;
- to be familiar with the audit objective and tests of control for each of the nine general control areas;
- to understand the auditing techniques that are used to verify the effective functioning of application controls; and
- to understand the auditing techniques used to perform substantive tests in a CBIS environment.

Notes

I. Attest Services versus Assurance Services

Because AIS is a prerequisite to the auditing course on many campuses, it is understandable that you not be too sure of the nature and purpose of an ***audit***. This introduction is, of necessity, brief. It will not take the place of your auditing course. But it is a start. Read carefully to distinguish between traditional auditing (the *attest* function) and the emerging field of *assurance services*. **Fig. 17-1, on page 861,** is a schematic of the relationship.

A. What is a Financial Audit?

Auditing is a form of *independent* attestation (or verification) performed by an *expert* who expresses an *opinion* about the *fairness* of a company's financial statements. Independence is of great importance since it is fundamental to stakeholder confidence in the audit opinion.

Conduct of an audit involves studying the client organization, evaluating the internal controls of the system to see how it works, and evaluating the information in the system.

B. Auditing Standards

You are familiar with GAAP, Generally Accepted Accounting Principles. These must be followed by companies required by SEC regulation to provide financial statements. In order for users to be confident that the audit did examine the books thoroughly, the external auditor must follow *GAAS, Generally Accepted Auditing Standards*. This section introduces GAAS, in particular, the *Statements on Auditing Standards* issued by the AICPA as needed, since 1972. Early in the text you were introduced to SAS 78. Read carefully the discussion related to **Table 17-1, on page 863.**

C. External Auditing versus Internal Auditing

Many of the same tasks are often carried out by external auditors and by individuals who are employees of the client. These employees who are involved in audit-related activities are called *internal auditors*. Although employed by the client firm, many duties can be conducted with a reasonable level of objectivity if the internal auditors report to the *audit committee* of the board of trustees, and not to the controller, who is responsible for the accounting system. Rather than representing the interests of

Notes

external stakeholders, they serve the best interests of the client organization itself.

Your text presents the standard definition of auditing and discusses the key elements. This is brief but good.

D. What is an Information Technology (IT) Audit?

IT auditing refers to the part of an audit that involves the computerized elements of an accounting information system. It is here that the elements of auditing are present. Note in particular, the discussion of audit objectives. **See Table 17-2, on page 866.**

E. The Structure of an IT Audit

Fig. 17-2, on page 867, is a schematic of an IT audit showing three phases: audit *planning*, *tests of controls* (tests of the system), and *substantive testing* (tests of the data in the system). Each of these phases is comprised of several steps. The discussion is clear.

II. Assessing Audit Risk and Designing Tests of Controls

Several concerns face an auditor–that material errors ***do*** exist in the accounting system and that the audit will ***not*** detect them. The text discusses ***audit risk***–the probability that an auditor will render a clean audit opinion when material errors exist.

A. Audit Risk Components

There are three basic components of audit risk:

- *inherent risk,*
- *control risk,* and
- *detection risk*.

There are two basic types of audit tests: ***tests of controls***, which determine whether the internal controls are operating correctly (i.e., these are tests of the accounting system), and ***substantive tests***, which determine whether the data fairly reflects the organization's financial affairs (i.e., these are tests of the accounting information in the system).

Notes

B. Relationship between Tests of Controls and Substantive Tests

The results of the tests of controls have great impact on the extent of substantive testing required. If the internal controls system is judged to be strong, less substantive testing is needed. Or, if the controls are deemed to be weak, more testing must be done to judge the data.

III. Tests of General Controls

This section of the text follows the framework developed in Chapter 15 with regard to general controls. The next section focuses on application controls. But first, you must understand the concept of an ***audit objective***.

A. Developing Audit Objectives

The objective(s) of any audit test relates to the exposures that may threaten the organization's activities and the internal controls that are in place. The approach that will be taken will relate *risk, control, the audit objective,* and the appropriate *audit procedure.* Significant professional judgment is required in practice.

Table 17-3, on pages 870-01, summarizes exposures and controls in a CBIS environment. Use this as your guide for reading the related narrative. For each area of control, the objectives and procedures are presented.

B. Testing Operating System Controls

Recall the objectives of operating system that we discussed in Chapter 15. The relevant control techniques are intended to verify that policies are strong enough to protect the operating system. These controls appear quite rigorous. But one disaster will make you a believer. The audit objectives and audit procedures are presented for each of five areas: *access privileges, password policy, virus control, audit trail controls,* and *fault tolerance.*

C. Testing Data Management Controls

Data management controls are comprised of ***backup controls*** and ***access controls***. The need for both should be clear.

Notes

D. Testing Organizational Structure Controls

We have discussed several times the fact that the *location* of separation of duties shifts in the CBIS environment. This is reflected in the tests examined here.

E. Testing System Development Controls

This type of control is extremely important for confidence in the output of the system. Not only must procedures be followed throughout the SDLC, but the system must have been justified and documented. The **review of SDLC documentation** is a good check on the *process itself*.

F. Testing System Maintenance Controls

The seventh stage of the SDLC is system maintenance. During the system's life, things often need to be changed. Just as the recording of financial transactions should only happen if *authorized*, changes in an existing system, i.e., *system maintenance*, should occur only with proper authorization and under strict control–in order to protect **system integrity**. The techniques discussed assume some programming knowledge.

G. Testing Computer Center Security

The objectives of computer center security should be obvious, by now. The tests that must be made will not be very exciting, but without the computer center, most firms would be unable to conduct business and would soon close their doors. This is true both from physical construction and backup power to full scale **disaster recovery**. Note the importance given to *critical applications*, first discussed in Chapter 15. The disaster recovery plan must be tested often because of changes in the organization, the environment, the system, and the personnel involved.

H. Testing Internet and Intranet Controls

There is little point in communicating electronically if the information is not transferred correctly or if it can be easily intercepted. Communication controls are designed to assure accurate communication, prevent unauthorized access, and make any data that is intercepted worthless.

Notes

I. Testing Electronic Data Interchange Controls

The value of EDI has been discussed before. If it is of benefit to trading partners, it is worth protecting. *Authorization, validation,* and *access* are key factors. With the absence of a paper trail, the issue of the *audit trail* deserves special attention.

J. Testing Personal Computer Controls

The problems inherent in the personal computer environment should not be underestimated. There is a connection with *end-user controls* that were discussed in Chapter 16. The text focuses on three areas of concern that are of special importance in the personal computer environment: *access, segregation of duties, backup*, and *systems development and maintenance.* Read this carefully. You will work in organizations "littered" with personal computers.

IV. Testing Computer Applications

The last area of exposure to be considered involves *application controls*. All that has been covered up to now related to *general controls*. Application controls fall into two classes: *tests of application controls*, and *tests of the transaction details and account balances*. The latter are *substantive tests* and are covered in the next section of the chapter. Tests of controls are considered below.

When computerized, or automated, accounting systems first made their entrance into the business world, auditors were frequently faced with a "black box" that they did not understand but which processed much of the data about which they were asked to voice an opinion. Initially they "audited *around* the computer" by observing input and observing output and checking for mutual consistency. Although adequate, it was nonetheless inefficient. Also, the evaluation of the internal control system was hampered. It was often impossible to trace an *audit trail* through the automated parts of the system. If an application had a material effect on the financial statements, auditing around the computer may not have been acceptable.

The second approach to auditing computer systems has been called *auditing through* the computer. It requires the ability to trace transaction paths from input to output through all parts of the system–manual and automated. The flow of data must be verified as it moves through the system, and the contents of machine readable files must be examined. Internal controls are tested *as they operate on the data*. The black box is gone.

Notes

The current trend is toward *auditing with the computer,* using the computer as a *tool* of the audit. The computer is used as a tool for examining the data, accessing the files, retrieving records at will, extracting statistical samples, and performing test calculations. Use of the computer has made feasible a great many procedures which would otherwise have been impractical from a clerical standpoint. The major problem that this last method creates is that practicing auditors are required to have extensive and up-to-date knowledge of computer systems. It is difficult to stay abreast of changes in technology. This has created a new demand for continuing professional education.

A. Black Box Approach

Note the advantages and disadvantages of this approach.

B. White Box Approach

Auditing *through the computer* can be called the "white box approach" to contrast it to the "black box approach." A number of tests of controls are discussed. The purposes of these different tests will help you appreciate the concerns faced by an auditor.

C. White Box Testing Techniques

Five proven procedures are described:

- *test data method*
- *base case system evaluation,*
- *tracing,*
- *integrated test facility,* and
- *parallel simulations.*

These are very complex techniques. Focus on the key objectives. The first three are variations of the same method. They all work *through the computer*. The last two actually use the computer as a tool of the audit–*auditing with the computer*.

D. The Integrated Test Facility

The ***integrated test facility*** builds auditability *into* the system. Both the logic of the application and the controls are tested during normal operation. The computer is now part of the audit process–the audit is being done *with the computer*. Focus on the advantages and disadvantage of this method. You will learn more about it in your auditing course.

Notes

E. Parallel Simulation

Parallel simulation, as the name implies, imitates the application under review. It must be written to perform the same steps as the application so that results can be compared. If the "real" system and the parallel yield the same output, then you would have confidence that the "real" system is OK.

V. Substantive Testing Techniques

The second major type of audit tests, after the *tests of controls*, are the *substantive tests* which are used to verify the $$$$ on the financial statements and in the accounts. Several examples are given in the text. Because these tests evaluate the data in the system, there must be ways to get at it.

A. The Imbedded Audit Module

The ***imbedded audit module*** is a set of specially written computer instructions built into the client software to extract specified types of data for later testing. Read through the advantages and disadvantages carefully.

B. Generalized Audit Software

Generalized audit software refers to a number of programs developed as tools for auditors. Because of the need to repeatedly perform basic audit tasks, many public accounting firms have created such packages. The text describes the type of functions built in. Concentrate on the tasks that can be performed by GAS, not the access to file structures.

Review Questions for Chapter 17: 1-29

Discussion Questions for Chapter 17: 1-16