CHAPTER 15

CONTROLLING COMPUTER-BASED INFORMATION SYSTEMS, PART I

The basic topic of internal control was introduced in Chapter 3. These next two chapters discuss the implications of automating the accounting information system on the need for and methods involved in internal control. The text identifies ten areas of control exposures. Six are discussed in this chapter, the remaining four in Chapter 16.

All of the discussion is presented following the framework of SAS 78.

The objectives of this chapter are:

- to understand how the unique features of a CBIS environment must be taken into account to achieve the control objectives specified in SAS 78;
- to be able to identify the principal threats to the operating system and the control techniques used to minimize the possibility of actual exposures;
- to be familiar with the various techniques used to control access to the database;
- to understand the nature of incompatible functions in a CBIS environment;
- to be familiar with the controls necessary to regulate systems development and maintenance activities; and
- to be familiar with the controls and precautions required to ensure the security of an organization’s computer facilities and with the recovery option available in the event of a disaster.
I. Effects of CBIS on the SAS 78 Control Framework

The discussion of internal control in a computer-based information system follows the framework presented in SAS 78—again with the addition of a sixth class: supervision. The objectives of internal control do not change. They still involve four broad objectives:

- to safeguard the assets of the firm;
- to ensure the accuracy and reliability of accounting records and information;
- to promote efficiency in the firm’s operations; and
- to measure compliance with management’s prescribed policies and procedures.

What does change in the CBIS environment is the manner in which the controls are implemented. The computer often does a combination of tasks that would be in “conflict” if done by the same person—at no risk. But other areas become concerns that did not exist in a manual system.

A. Transaction Authorization

The difference in operation that the CBIS environment can yield is shown in the example of authorizations. The fact that the computer authorizes transactions following the steps built into the program is not a problem if the controls over the programs themselves are adequate.

B. Segregation of Duties

As noted in the text, since the computer will not collude with itself to jeopardize the organization, combining otherwise incompatible tasks in a program is not an issue. However, the concern for segregation of functions shifts to the system development process. The tasks of program development, program processing (operations), and program maintenance must be adequately segregated so that improper, unauthorized changes cannot be made.

C. Supervision

When the segregation of duties cannot be religiously adhered to, the best alternative is supervision. Note the fact that even this approach assumes that employees are competent and honest. In a manual environment, issues of span of control are relevant. In a CBIS setting, a third issue, location disparity, adds
a new wrinkle. The way in which supervision occurs must change.

D. Accounting Records

In the area of accounting records, the difference between manual and automated systems is “apparent.” The paper is reduced, if not totally eliminated. And with it can go the audit trail, which must now be built into the CBIS.

E. Access Control

The issue of access is multifaceted. On one dimension is the issue of direct and indirect access. In a paper-based system the records existed somewhere. The ability to copy electronic files easily means that the records can exist everywhere. This makes control much more difficult. The text also discusses concerns with fraud and disasters.

F. Independent Verification

The double checking that is inherent in a manual system to detect arithmetical and clerical errors provided other forms of verification. With automation, arithmetic errors do not occur, nor do transposition errors. The role of independent verification now shifts to the systems development and maintenance activities.

II. General Control Framework for CBIS Exposures

The text presents an approach to control in the CBIS environment that classifies exposures into ten categories or topics. The discussion follows this framework. Areas one to six are covered in this chapter, and seven to ten in Chapter 16. Some of these are more important for accountants than others, but you should be aware of the main issue in each category.

The AICPA views internal control as being of two types: administrative (e.g., hiring policies) and accounting (accuracy of data). Within accounting, they are further broken down into general (applying to many, if not all parts of the system; e.g., computer center access) and application (which relate to a specific application; e.g., in a payroll system, no employee time card should report more than x hours of work in a week).

In the following discussion, topics one through nine all involve general controls. Only topic ten, as its name indicates, involves application controls.
Table 15-1, on page 771, is an excellent summary of the first six areas of exposure and control in a CBIS environment.

III. Operating System Controls

This section does a good job of explaining the role of the operating system and the ways in which it can be threatened. The objectives of operating system control should not surprise you, though they can appear quite humorous.

A. Operating System Security

Operating system security is focused on who can access the operating system, which resources (files, programs, printers, etc.) they can access, and what they can do. Several key components of operating system security are discussed:

- log on procedures, you should be familiar with user IDs and passwords;
- access tokens, internal information used to approve actions;
- access controls, which list who can do what; and
- discretionary access control, which gives users in distributed systems specific powers.

B. Threats to Operating System Integrity

This section is very important. The operating system is threatened by both accident and intent. Intentional threats include intentionally destructive programs.

C. Operating System Control Techniques

This section is quite technical for non-systems professionals. It discusses various control techniques. (Keep the SAS 78 control areas in mind.)

- controlling access privileges;
- password controls include several options; such as reusable passwords and one-time passwords;
- controlling malicious and destructive programs;

If you have not had any exposure to the techniques that can be used, beyond knowing the word “virus,” read this carefully. In the popular press, the word “virus” is used broadly to describe many types of nasty software, including worms, Trojan horses, logic bombs, etc.
Computer viruses are a fact of life. Read carefully—if only in self-defense. Software access procedures are important. This may explain some “absurd” policies that prohibit personal software (like games) on company computers and prescribe operating rules in your college computer labs.

- **system audit trail controls**: As accountants you value the audit trail. This section discusses various techniques used.
- **audit trail objectives**;
- **implementing the audit trail**; and
- **fault tolerance controls**.

### IV. Data Management Controls

Organizations store data because it has value and will be useful in the future. These reasons for storing data create some concerns. If it has value, it should not be available to just anyone—access should be controlled. If it will be useful or needed in the future, it must be available—backups must be assured.

#### A. Access Controls

Because of the “shared” nature of database management systems, **access control** becomes an issue in this setting. The discussion is complex, but do grasp the importance! The discussion of passwords, encryption, etc., will be informative. Pay attention to **inference control**, especially the example.

#### B. Backup Controls

If the other controls fail, an organization still must function. Most database systems use a backup system like the one shown in Fig. 15-3, on page 780. Note the parts of the system: database backup, a transaction log, checkpoints, and a recovery module.

### V. Organization Structure Controls

We have mentioned above that the importance of segregation of duties in a CBIS environment is shifted to the systems functions. This section looks at how this should be addressed in two possible settings: a firm with centralized computer services and one with a distributed arrangement. The concerns are the same, the approach different.
A. Segregation of Duties Within the Centralized Firm

With regard to the segregation of duties in a CBIS, the key points are to:

- separate systems development from computer operations—people who write programs don’t run them. This provides a double check if, for example, duplicate checks were printed;
- separate database administration from other functions; and
- separate new systems development from maintenance

Note the organizational structure shown in Fig. 15-4, on page 781. Development and maintenance are separate.

B. The Distributed Model

When efficiency and other factors lead to distribution of computer services across an organization, adjustments must be made. Several control implications are discussed—such as different departments using different software, etc. These issues are real. When computers (PCs) began to proliferate in organizations, things happened without thought. Department A bought Lotus and department B bought Excel, etc.

C. Creating a Corporate Computer Services Function

The concept of a corporate computer services function to support distributed computing is presented. It aims for the best of both worlds: user ownership and professional support capability.

VI. Systems Development Controls

Although accountants do not develop systems, their confidence in the output of the system requires that they be confident that control is adequate.

A. Controlling New Systems Development Activities

Six activities within development and related controls are discussed. Auditors are concerned about the use of client resources as well as the integrity of the resulting system.
B. Controlling Systems Maintenance Activities

A great deal of attention is focused on the systems development activities. Once the system is up and running, it is easy to assume that all is well. Remember the iceberg! Several areas requiring serious control are mentioned: authorization, testing, documentation and source program library controls.

The concept of a source program library is introduced. The focus is on the importance of controls, with counter-examples.

VII. Computer Center Security and Controls

The best laid plans of mice and men . . . No matter how good the controls are, something can go wrong. Two areas are discussed, computer center controls, which are preventive, and disaster recovery planning, which is corrective.

A. Computer Center Controls

Don’t build a china factory on the San Andreas Fault. And don’t put a big computer in a basement that floods often; use fire-proof materials, etc.

B. Disaster Recovery Planning

The planning for recovery must occur before the disaster, not after. Several approaches to disaster planning are presented. None are fool proof. What ever is done should be tested in advance. Pay close attention to the issue of identifying critical applications. The system is supposed to help the organization meet its objectives. Who decides what is critical? What would an organization need to do first to resume business after a fire?

Review Questions for Chapter 15: 1-19, 23-30
Discussion Questions for Chapter 15: 1-4, 8, 11-16, 19