CHAPTER 3

ETHICS, FRAUD, AND INTERNAL CONTROL

The three topics of this chapter are closely related. ***Ethics*** is a hallmark of the accounting profession. The principles which guide a manager's decision making are important to all affected. *Computer* ethics involves questions related to the use of technology and its social impact.

Fraud is a serious problem for most businesses today and often technology compounds the problem. In addition, the role of the independent auditor in the detection of fraud is often questioned.

Because managers and accountants need to be confident that the information produced by the accounting system is both accurate and reliable, the importance of ***internal control*** is great.

The objectives of this chapter are:

- to understand the broad issues pertaining to business ethics;
- to know why the subject of ethics is important to the study of accounting information systems;
- to have a basic understanding of ethical issues relating to the use of information technology;
- to be able to distinguish between management fraud and employee fraud;
- to be familiar with the common fraud techniques used in both manual systems and computer-based systems;
- to be aware of the gap that exists between the expectations of users of financial statements and the ability of auditors to detect fraud;
- to understand the internal control structure defined by SAS 78; and
- to recognize on a fundamental level the implications of the use of computer technology for the internal control structure.

Notes

I. Ethical Issues in Business

The first part of this chapter gives a very simple introduction to the subject of business ethics. Hopefully ethical questions have been addressed in many of your business courses, especially your accounting courses. Ethics ***do matter***. Any accounting student who does not agree is in the wrong major!!!

A. What is Business Ethics?

Table 3-1, on page 119, identifies various business decisions which have ethical dimensions. These are grouped according to the four areas of ***equity, rights, honesty,*** and ***exercise of corporate power***. Many situations in accounting, even related to the structure and content of systems, raise ethical questions. Students must understand how managers determine what is right in doing business and how they achieve it.

B. How Some Firms Address Ethical Issues

Ethical behavior is the antithesis of the "dog-eat-dog" approach to doing business. The importance of management setting the tone and supporting an ethical climate cannot be overstated. As is true of many other management philosophies, it is lower-level managers who must carry out management's directives. Subordinates who feel that an organization's commitment to ethical behavior is lacking should start job-hunting.

Fig. 3-1, on page 121, is a representation of behavioral stage theory which shows the levels of moral development. Where are you?? Read this material carefully.

C. What Is Computer Ethics?

This discussion of *computer ethics* is very well done. Note in particular the meaning of *pop, para*, and *theoretical* computer ethics. Much has been written on this topic. Some of you may be surprised by some of the issues that arise from the adoption of a new technology. The significant areas include:

- privacy,
- security, including accuracy and confidentiality,
- ownership of property,
- race,
- equity of access,

Notes

- environmental issues,
- artificial intelligence,
- unemployment and displacement,
- misuse of computers, and
- internal control responsibility.

II. Fraud and Accountants

One of the reasons, though not the only one, for the discussion of ethics is the reality of its **absence**. Reports of various occurrences of fraudulent behavior are commonplace in the press. It appears that ***fraud*** is widespread. Your text discusses two types of fraud, *management fraud* and *employee fraud*, and presents several motivating factors.

The Concept of Fraud

Despite the fact that the purpose of a financial statement audit is to attest to the fairness of the financial statements ***prepared by management***, the public and other groups often want to blame the auditors when fraud goes undetected.

Your book does a good job of defining and discussing fraud as it has evolved in common law. For an act to be regarded as fraudulent, five conditions must be present:

- *false representation* [some misrepresentation or omission must have occurred],
- *material fact,* [it must matter],
- *scienter,* [there must be the intention to deceive],
- *justifiable reliance,* [it affected someone's decision], and
- *injury or loss* [must have occurred].

Our discussion will focus on two forms of fraud which impact businesses: *management fraud* and *employee fraud*. The distinction is important.

Employee fraud usually involves the stealing of firm assets. The book discusses it in three steps: take, sell, and hide.

Management fraud is a fraud committed not to directly line the pockets of the perpetrator, but to present an overly optimistic picture of the firm in order to enhance share price or to obtain more favorable financing. Several factors are particularly important:

1. It usually occurs at levels **above** the normal internal control system.
2. There is typically an intent to present a better picture than is valid.
3. If assets are misappropriated, the rout is quite devious.

Notes

A. Factors that Contribute to Fraud

After presenting the results of a study by Certified Fraud Examiners (CFE), your book discusses the types of forces which can interact to inspire an otherwise responsible person to commit fraud: situational pressures, availability of opportunity, personal characteristics. Read this material carefully.

Another approach to explaining fraud lists three conditions:
1. necessary skills,
2. opportunity, and
3. a non-shareable problem.

Prevention of fraud by external auditors is very difficult. Detection can occur if certain questions are asked. See the discussion in the text.

B. Financial Losses from Fraud

Much information is reported from a 2002 study by the Association of Certified Fraud Examiners. First is a discussion of the magnitude of losses. The following sections describes the characteristics of perpetrators.

C. The Perpetrators of Frauds

This section will be an eye-opener. Read carefully the narrative that accompanies **Tables 3-2 to 3-7, on pages 129-131.** In particular, consider the issues of gender, position, age, education, and collusion.

D. Fraud Schemes

The discussion of types of fraud is organized following the CFE categories: fraudulent statements, corruption, and asset misappropriation. Many examples are given. Regard this material as an eye opener – not a "how to" chapter!

The issue of fraudulent statements should be very familiar, given the recent notoriety of Enron, WorldCom, and Adelphia. Four issue are key: lack of auditor independence, lack of director independence, questionable executive compensation schemes, and inappropriate accounting practices. This leads to an excellent discussion of the *Sarbanes-Oxley Act* passed in July 2002.

Fig. 3-3, on page 139, is a standard model for an AIS. The discussion of computer fraud techniques

Notes

looks at the types of fraud possible at each of the stages in the system:

- *data collection (input),*
- *data processing,*
- *database management (storage)*, and
- *information generation (output).*

III. Internal Control Concepts and Procedures

Although it has always made sense for management to want to ***control*** operations to make sure that plans are carried out and objectives achieved, it is also **law** that a system of internal control be set up and maintained. The Foreign Corrupt Practices Act of 1977 mandates what common sense has always recommended.

A. Internal Control in Concept

The objectives of an internal control system cover the entire firm, not just the AIS. They should not be surprising:

- 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.

Obviously, all things cannot be assured at 100% without bringing an organization to a halt. Hence your text discusses some modifying assumptions: *management responsibility, reasonable assurance, methods of data processing,* and *limitation on effectiveness.*

Read carefully the discussion of exposure and risk. ***Exposure*** is defined as the absence or weakness of a control that increases the firm's chance of a loss. ***Risk*** is the likelihood of such loss. Firms invest in internal control systems to reduce exposures and/or risks. **Fig. 3-4, on page 145,** is a nontraditional way of viewing the relationship between undesirable events, exposures, internal control, and assets.

Notes

Fraud is not the only concern that internal control is designed to address. Unauthorized access to assets (especially information), errors due to human or machine slip-ups, and mischief (including computer viruses, etc.) are also the targets of internal control.

Fig. 3-5, on page 146, represents a common view of controls, the **PDC control model**, which classifies controls as to when they occur relative to the "problem." ***Preventive*** controls are implemented before a problem, to prevent its happening. ***Detective*** controls identify problems that have occurred. ***Corrective*** controls attempt to repair the damage.

B. Auditing and Auditing Standards

Read carefully the discussion of ***generally accepted auditing standards (GAAS)*** presented in the text and summarized in **Table 3-9, on page 148.** Recognize that these ten standards will take on greater meaning when you take your auditing course. These serve here as a guide. Of particular importance is Statement on Auditing Standards #78.

C. Internal Control Components

Internal control has five components.

1. The *control environment* is the atmosphere created in the organization in support of control objectives. The other four assume this environment.

2. *Risk assessment* is a necessary part of management's effort. It must identify, analyze, and manage risks, not just hope that nothing goes wrong.

3. *Information and communication* are the basis of the accounting information system. It is crucial that the quality of the information generated be secured.

4. Having a system of internal control is a start. *Monitoring* the system to assure that the internal controls are functioning properly is required.

5. *Control activities* are outlined in SAS 78. There are two categories: computer controls and physical controls. [Computer controls are the topic of Chapters 15 and 17.] Of particular importance is how the controls are

Notes

different in computerized systems, compared to manual. The discussion will be organized according to six traditional areas of control:

a. **Transaction authorization**: only valid, approved transactions should be recorded.

b. **Segregation of functions**: the same person should not be responsible for authorization, recordkeeping, and custody of assets.

c. **Supervision**: when there are too few individuals to implement total segregation, the *compensating* control is good supervision.

d. **Accounting records**: implies the design and use of adequate documents and records to help ensure the proper recording of transactions and events.

e. **Access controls**: assures that access to assets is permitted only in accordance with management's authorization (this refers to both physical and logical assets). Again, the integrity of the audit trail is the concern.

f. **Independent verification**: to check on the performance of individuals, the integrity of processing, and the correctness of data.

D. The Importance of the Internal Control Structure

As part of the preparation for a financial statement audit, the auditors must ***evaluate the system of internal control***. This must occur before the planning of the rest of the audit.

Review Questions for Chapter 3: 1-7, 19-21, 24-29, 31, 32, 36-38.

Discussion Questions for Chapter 3: 3-5, 8, 9, 11-32.

