Chapter 1

INTRODUCTION

LEARNING OBJECTIVES

After completing this chapter, you should be able to do the following:

- Determine the general warning signs of fraud.
- Identify characteristics of individuals that perpetrate financial statement fraud.
- Identify general techniques to prevent, detect, or deter fraud.

Overview

This course is designed to give auditors and accounting and finance professionals an understanding of where in the government and not-for-profit environments fraud typically occurs and how to recognize and respond to these risks. With this knowledge, management of governmental or not-for-profit entities is in a better position to develop fraud programs and controls that will be effective in responding to fraud risks. Likewise, such understanding improves the likelihood the auditor of governmental and not-for-profit entities will identify and properly respond to the risk of material misstatement due to fraud.

In short, the purpose of this course is to address how management of governmental and not-for-profit entities and their auditors can recognize and respond to fraud risks that are unique to these entities.

Key Point

Throughout this course, the terms *he* and *she* are used alternately and no discrimination or implications related to either gender is intended. Additionally, this course and its appendixes have been developed using the professional and industry standards, practices, and procedures in effect at the time of the writing. Management, auditors, and other professionals should consult current authoritative guidance in addition to these materials.

Introduction

In the early years of the twenty-first century, the accounting profession experienced some of its darkest days since the 1938 McKesson-Robbins corporate accounting scandal. Massive scandals in the early 2000s at Enron, WorldCom, and Global Crossing put all CPAs in the spotlight whether they were auditors of publicly traded companies or small, closely held family corporations. To protect the American public against such spectacular failures in the future, President George W. Bush signed the Sarbanes-Oxley Act (SOX) into law in the summer of 2002.

It is interesting to note that whereas Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*), which is now clarified and codified as AU-C section 240, *Consideration of Fraud in a Financial Statement Audit* (AICPA, *Professional Standards*), was released after the passage of SOX, it was not issued in response to the failures giving rise to its passage. SAS No. 99 was the result of a four-year process that began with five academic research studies conducted as part of the AICPA Fraud Research Steering Task Force. In addition to these studies, the Public Oversight Board, at the request of the Securities and Exchange Commission, appointed a Panel on Audit Effectiveness in 1998. This Panel conducted its own research primarily related to audit effectiveness and issued a report in August of 2000.

Using these studies and other information, the AICPA Fraud Task Force, established in September of 2000, reviewed the previous guidance in SAS No. 82, *Consideration of Fraud in a Financial Statement Audit*, and concluded it was fundamentally sound. The recommendations of this task force to enhance professional auditing standards related to fraud were incorporated in the exposure draft issued February 28, 2002, which was adopted as SAS No. 99 in October of 2002 and later clarified and codified in AU-C section 240.

Fraud has become a major focus among not only financial statement users but also among many Americans in their roles as investors, watchdogs, philanthropists, or private citizens. In the last several decades, news reports have often revealed fraud and abuse at all levels of governmental and not-for-profit organizations. The national-level United Way scandal of the early 1990s had a significant negative impact on many local United Way agencies. Americans were outraged to learn the federal government had spent thousands of dollars for items that could have been found at the local building supply store for less than $100. Citizens of Dixon, Illinois were shocked to learn of the massive fraud perpetrated by a long-term high-level employee whose family had been a member of the community for generations.

Individuals and businesses contributing to not-for-profit organizations have a legitimate expectation that their donations will be used to further the mission of the not-for-profit organization. When such funds are diverted for other uses, or worse, appropriated for personal gain, the reputation of the not-for-profit organization is jeopardized. In such cases, the lack of trust potential individual and corporate donors have in the not-for-profit organization can seriously affect its revenues and, correspondingly, its continued existence.

For citizens, fraud in governmental organizations is a misuse of the public funds they provided to the government without choice and in good faith. Such breaches of trust further erode their tenuous faith in the "American Way" and needlessly increase the cost of providing public goods and services. Simply put, everyone loses when fraud occurs in governmental organizations.

General Warning Signs of Fraud

Being aware of situations that have the potential to create fraud risks is the first step in designing effective programs and controls to prevent, detect, and deter fraud. The following general situations may be warning signs indicating fraudulent financial reporting or fraud due to misappropriation of assets:

Warning Signs	
Warning!	An organizational culture of arrogance and management entitlement
Warning!	Accounting policies that rely too heavily on management's judgment
Warning!	Accounting policies that seem too aggressive, especially in light of accounting and finance staff expertise
Warning!	Overly centralized control over financial reporting, especially in organizations with larger or more adequate staff in the areas of accounting and finance
Warning!	Departure of key senior management personnel
Warning!	Failure to listen to key accounting or finance personnel within the organization
Warning!	Receivables growing at a faster rate than the related revenues
Warning!	Periods of prolonged success especially when economic, industry, or organizational conditions indicate otherwise
Warning!	Difficulty in paying bills on a timely basis or less timely than in prior years
Warning!	Transactions lack economic purpose (may be indicative of kickbacks as well as misappropriation of assets or financial statement fraud)

KNOWLEDGE CHECK

1. Which is NOT a general warning sign of fraud?

   a. Organizational culture of arrogance and management entitlement.

   b. Overly centralized control over financial reporting.

   c. Open and honest communication between key accounting or finance personnel and top management of the organization.

   d. The entity engages in transactions that lack economic purpose.

Ways to Prevent, Detect, or Deter Fraud

A number of low-cost, high-impact policies and procedures can be implemented to help prevent, detect, and deter fraud in most governmental and not-for-profit organizations. A highly effective and almost no-cost control that can be implemented by any governmental or not-for-profit organization is to *take a hard line* with respect to fraud. If the "tone at the top" is one of zero tolerance and fraudsters are promptly disciplined, employees may be less likely to commit fraud. A *positive and open work environment,* at all levels of the organization, also helps in preventing, detecting, and deterring fraud.

To design effective fraud prevention programs and controls, it is necessary to understand what type of individual typically perpetrates fraud. Fraud research consistently indicates the common characteristics of individuals that perpetrate financial statement fraud are

- a trusted employee,
- dedicated and often works long hours,
- dislikes mandatory vacation policies,
- resents cross-training,
- seen as likeable and generous, and is
- deceptive and usually an adept liar.

General Techniques to Prevent, Detect, or Deter Fraud

Other general techniques to prevent, detect, or deter fraud include the following:

- *General*
    - Periodic review of control accounts for adjustments when fully integrated subsidiary systems are in place
    - Establishment of a "fraud hotline" (as simple as a board member with a cell phone or as sophisticated as a separate phone line allowing anonymous calls on any day and at any time)

- *Cash*
    - Timely reconciliation of and review of bank statements for
        - unusual activity,
        - dual endorsements on back of checks,
        - changes to items on front of checks, and
        - individuals endorsing checks issued to a business

- *Purchasing/ accounts payable*
    - Extensive paperwork and procedures related to setting up new vendors (especially effective if purchasing is extremely decentralized)
    - When controls and programs related to cash disbursements or purchasing are inadequate, use of a simple software program (internally developed or purchased off the shelf) to
        - cross-reference vendor names to all permutations of employee names;
        - cross-reference vendor payment addresses to all employee addresses;

    - cross-reference all delivery locations on vendor statements to all physical addresses of the organization;
    - cross-reference phone numbers on vendor statements to employee phone numbers;
    - cross-reference all delivery locations on vendor statements to all employee addresses;
    - identify vendors with higher than expected purchase volume either for the month or for the year (or some other meaningful period);
    - identify transactions (purchases, purchase orders, and checks) falling just below established threshold amounts listed by vendor, purchaser, department/ agency, employee, etc.;
    - list vendors with incomplete master file information; and
    - list vendors added and deleted within an established time frame.

- *Payroll/personnel*
    - Mandatory background checks prior to starting work
    - Printing accrued and unused leave hours on employee pay check stubs (deters theft of hours when payroll/ personnel controls are inadequate)
    - Surprise visits to offsite locations

COMPUTER FRAUD

In today's business environment, technology plays a major role in almost all aspects of an organization's operations. The auditor or chief financial officer may be unable to keep up with technological changes. In many of these cases, the establishment of programs and controls to prevent, detect, or deter computer-related fraud is left to the technology function. By understanding the factors that encourage fraud, effective programs and controls that discourage fraud can be developed.

Factors influencing computer crime are either motivational or personal. Motivational and personal factors relate to both rationalization/ attitude and incentive/ pressure in the fraud triangle. The following motivational and personal factors tend to encourage computer fraud:

- Inadequate pay and benefits, including promotional opportunities
- Poor communication of expectations (job performance, behavior, and the like) by management
- Lack of performance feedback mechanisms
- Mediocre performance as an acceptable performance standard
- Inadequate support and lack of resources to meet standards
- Not enough review and follow-up to assure compliance with organizational programs and controls
- Inadequate standards of recruitment and selection
- Deficient or missing orientation and training programs

Preventing computer fraud is not necessarily a highly technical or expensive proposition. The primary factors that discourage computer crime are

- internal accounting controls,
- access controls, and
- Internet firewalls.

Preventing, Detecting, and Deterring Computer Fraud
Separation and rotation of duties both within and external to the technology function
Timely update of accessible computer applications when personnel change jobs or when the requirements of their current position change
Periodic and surprise inspections and security reviews
All control policies and procedures required to be written (zero tolerance for deviations from this policy)
Offline controls and limits such as batch controls and hash totals where indicated and cost-effective

Access controls to prevent, detect, and deter computer fraud include the following:

- Authentication/ identification controls, such as
    - keys,
    - smartcards,
    - passwords,
    - biometrics,
    - callback systems,
    - one-time passwords,
    - constrained access by time and day, and
    - periodic code and password changes
- Compartmentalization of information
- Encryption of data while stored or in transit

Knowledge Check

2. Which is NOT a general technique to prevent, detect, or deter personnel fraud?

    a. Mandatory background checks prior to starting work.
    b. Routine visits to offsite locations.
    c. Printing accrued and unused leave hours on employee pay check stubs.
    d. Performance feedback mechanisms.

Summary

This chapter provided an introduction to fraud including general warning signs of fraud. Additionally, this chapter identified the characteristics of the "typical fraudster" and provided general ways to prevent, detect, and deter fraud. Also discussed in this chapter were general controls that can be implemented to address computer fraud risks.

Practice Questions

1. List three ways to prevent, detect, or deter computer fraud.

2. List three characteristics common to individuals that perpetrate financial statement fraud.