CHAPTER ONE

The Architect's Blueprint

Establishing the Framework

IN 1992, THE COMMITTEE of Sponsoring Organizations of the Treadway Commission (known as COSO), developed and issued a framework for internal control design. According to its website, www.coso.org, "the Committee is a joint initiative of The American Accounting Association, The American Institute of CPAs, Financial Executives International, The Association of Accountants and Financial Professionals in Business, and The Institute of Internal Auditors. COSO is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence."

The COSO internal control framework is a picture of the proper design of an internal control structure. It contains certain elements that must be included in developing internal controls as a part of an anti-fraud program. There have been certain modifications of the framework recently, but the overall elemental design has stood the test of time for more than 20 years.

THE ELEMENTS OF ANTI-FRAUD PROGRAM DESIGN

The original COSO framework outlines five elements of internal control design: (1) the control environment, (2) risk assessment, (3) control activities,

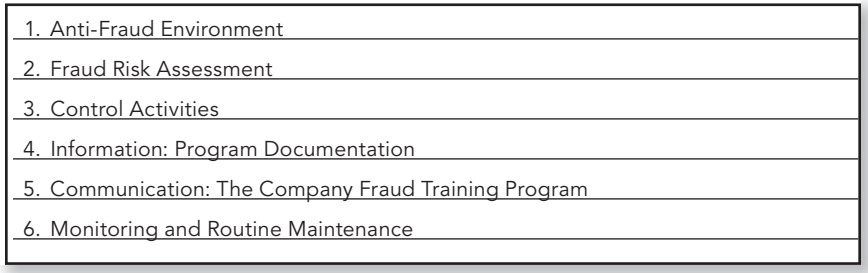

FIGURE 1.1 Revised Six Elements

(4) information and communication, and (5) monitoring. While keeping with the intent of this structure, I have modified the names and format of some of these elements to best present the architect's blueprint for the design process of the anti-fraud program. The revised six elements are shown in Figure 1.1.

Each reference to program design in this book includes a categorization of the guidance into one or more of these elements. As the elements are addressed, more specific definitions of each will be provided. However, a basic description of each element is provided next to familiarize you with the concepts.

ANTI-FRAUD ENVIRONMENT

The anti-fraud environment is best described as the tone at the top. What is the level of concern for fraud prevention from the business owner, the board of directors, or those bodies tasked with governance of the company? If there is no concern from these parties, assuredly there will be no concern from those below. Conversely, if the owners or governing bodies of a company exhibit an appropriate concern for fraud prevention, then the staff should follow suit.

Evidence of these concerns is demonstrated through the anti-fraud environment: the environment that includes processes and policies established to address fraud risk. Specific best practices for the proper design of a sound anti-fraud environment are presented throughout further sections of this book.

FRAUD RISK ASSESSMENT

In my experience, I have seen that fraud risk assessment is the most neglected of the six elements. I attribute this to the fact that fraud risk is a concept not dwelled on by most small business owners. Small business owners possess an

entrepreneurial spirit, the ability to cast a vision, an understanding of their product or service, and the ability to profit from these attributes. Fraud prevention, accounting, and risk assessment are delegated to the accountants. We all have our own set of gifts and talents that, when working together, provide the best operating results for a company.

However, the responsibility for an effective anti-fraud program lies with those with governing authority over the company. Those individuals may certainly seek the advice of the accountant types in designing the anti-fraud program, but the overall responsibility cannot be delegated away from the governing body.

To illustrate, let's look at one example of a risk assessment issue for a company. Assume Company A sells computer parts, such as chips and the numerous electronic insides of a computer. When considering the risk of fraud in a company like this, we would most likely focus on the sales, billing, and collection processes more than the inventory processes. The risk of fraud in the inventory area may be relatively low since electronic components, while costly in nature, are not necessarily susceptible to quick conversion to cash. Some rogue employee swipes a handful of computer chips. What can the employee do with them? Unless he happens to be a participant in a major underground market for these chips, he probably won't profit much in the way of cash. So the risk assessment team will focus less on inventory fraud risk and more on the sales, billing, and collection areas.

Conversely, Company B sells the computers that use Company A's chips and electronics. Now, when considering inventory fraud, there is a whole new level of risk. Company B has a warehouse full of laptop computers. These items are relatively small, fit in a backpack, and are easily converted to cash through sales on the street. A rogue employee carries off a couple of laptops in his backpack every day and sells them on the street for $500 each. That's $1,000 per day. Over the span of 20 working days per month, that adds up to $20,000, or $240,000 annually—which, in my opinion, isn't bad beans! Therefore, Company B's fraud risk is in inventory, whereas Company A's lies in another area entirely.

This type of thought process is necessary to understanding how to perform a fraud risk assessment. Because of the importance of this aspect of the framework, an entire chapter is devoted to this subject.

CONTROL ACTIVITIES

This element of internal control is represented by the actual checks and balances that exist. Control activities are *specific.* One of the most common is the bank reconciliation. The performance of the bank reconciliation is a major

business process that can also function as an outstanding control activity. If done correctly, bank reconciliations serve not only to prevent fraud but also to detect fraud. Requiring dual signatures on checks over a certain dollar amount and physical inventory counts are excellent examples of specific control activities. Their design is of such importance that I have devoted several chapters to control activities as they apply to various financial areas common in most businesses.

INFORMATION: PROGRAM DOCUMENTATION

In our journey to design the best possible anti-fraud program for your business, we have established a proper anti-fraud environment, assessed the areas of greatest fraud risk, and designed specific control activities to address those risks. Now we need to document that system.

The *information* aspect of this element speaks to the need to commit this program to written form. I consider myself moderately intelligent, but there is no way I would be able to memorize all of the aspects of an anti-fraud program. Committing all of this to written form sounds relatively simple, yet I constantly encounter companies whose anti-fraud strategies are known only by those performing the activities. What happens when these individuals are hit by the proverbial bus? Once they're gone, so is the program, because the replacements won't know it exists. While simple in concept, the process of documentation can become too complex very quickly. This book includes a separate chapter devoted to how to avoid the pitfall of overcomplexity. Remember our motto: *Simple practicality.*

COMMUNICATION: THE COMPANY FRAUD TRAINING PROGRAM

Once the program is in written form, it must be *communicated* to staff, to those who will be responsible for carrying out the program. Do we send out memos? Do we give everyone a binder? Do we have live meetings? Is the program posted on our intranet? Do we periodically conduct training for staff as to how the program works? Do we seek input on problems encountered in carrying out the designed controls? Yes. The answer is a resounding yes. All of these combined represent the best communication efforts. How to combine these efforts to achieve the most effective communication is addressed in further chapters.

Communication is important in both our personal and business relationships. My wife and I have been married for 30 years. Without proper communication, I'm not sure we could have made it this long. Suppose we left our wedding ceremony 30 years ago and never spoke again. That's ludicrous; that's silly to even think about. Yet, more companies than not treat the communication of the anti-fraud program exactly like this. The work is done. Someone said we had to do it. So we did it. We put it in the most beautiful binder imaginable! Then we proudly put it on the shelf and never looked at it again. That's ludicrous; that's silly to even think about.

MONITORING AND ROUTINE MAINTENANCE

The second most neglected element in anti-fraud program design is monitoring and routine maintenance. Monitoring is the built-in process of periodically determining compliance with all aspects of the anti-fraud program. If certain staff members are not complying with the controls in place, we should go the extra step and ask why. Is it a problem with the individual or with the design of the control? Regardless of how this question is answered, there is either someone or something that needs to be fixed.

An anti-fraud program is not a static program. It is a living, breathing document that needs to change based on operational changes. If we don't ever monitor the controls for effectiveness and efficiency, how will we know what needs changing?

Consider in our building metaphor that we have completed the construction of our new home. Obviously, we will move in and live there, possibly forever. Let's assume that through the years we perform no routine maintenance on this home. Eventually it will fall apart and lose all of its effectiveness as a home. Allowing this to happen to your home would be considered extremely irresponsible. The monitoring element of the anti-fraud program is essential to the accomplishment of routine maintenance. Without it, the program will eventually fall apart and lose its effectiveness as a program.

• • •

These six elements provide the framework into which everything we address from this point forward will fit. Think of this framework as the architect's blueprint for a new home. It is the plan for going forward. Without this plan, this blueprint, this framework, our structure will be unsound, ineffective, and possibly even dangerous.

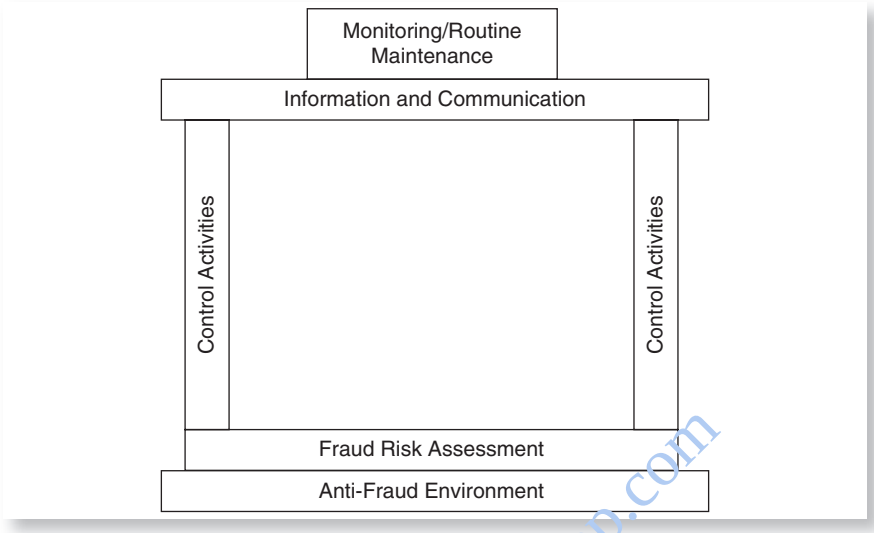

FIGURE 1.2 Framework

The *anti-fraud environment* is the foundation, the *fraud risk assessment* is the ground floor, the *control activities* are the walls (the structure), the *information and communication* elements tie it all together as the ceiling, and the *monitoring and routine maintenance* element tops it off under one roof.