

1

CHAPTER ONE

What Is a Fraud Audit?

THE DEBATE IS OVER; auditors have a responsibility to respond to the risk of fraud. The stockholders, board of directors, and management of organizations are looking to their internal auditors to detect fraud before it undermines the vital operations that are referred to herein as the core business systems. Auditing standards now require auditors to respond to the risk of fraud. Phrases such as *professional skepticism*, *identified fraud risk*, *fraud risk assessment*, and *fraud audit procedures* are now found in use within organizations of all types to meet the current standards. Unfortunately, this change seems to be an agonizing effort for all involved. Just say the very word *fraud* and everyone seems to react as though someone has contracted the bubonic plague. Therefore, all parties involved in the effective, efficient, and healthy operation of an organization, such as the aforementioned auditors and various stakeholders, need to recognize what fraud is, where it is found, and how it is found. So, when we speak of fraud in the context of auditing, it denotes a distinct body of knowledge, the mastery of which is needed to address the risk of fraud. The title of auditor does not immediately confer knowledge regarding fraud, and it certainly doesn't infer the mastery of identifying the risk. Auditors need to possess this specialized knowledge to solve the difficulties in addressing fraud that

2 ■ The Fraud Audit

perplex the profession. So, fear no more, because you, the auditor, aren't facing a steep climb up a mountain of knowledge all alone. No, the purpose of this book is to give you the guidance, strategy, and tools you'll need to make a safe trip.

The Awareness Theory Methodology (ATM) approach to fraud auditing is at the heart of our discussion of the fraud audit. The objective of "ATM" is to provide a conceptual framework for the fraud audit. Fraud theory (the "T" in ATM) asserts that fraud is a body of knowledge. Understanding the how, why, and where of fraud are critical elements of this body of knowledge. Knowing "how" fraud occurs is dependent upon a logical, rule-based system whereby the auditor identifies the fraud scenarios facing an organization. Consequently, a process must be provided for describing the fraud scenarios inherent to the core business system. The process is commonly referred to as the fraud identification stage. The "why" fraud occurs involves the reasons individuals commit fraudulent acts against an organization. Referring to the quintessential fraud triangle, the reasons for committing fraud relate to pressure and rationalization factors. Knowledge of the typical underlying reasons of why fraud is committed is critical to both building the control environment and enhancing an auditor's awareness to the likelihood of fraud. Last, the question of "where" fraud occurs is the premise of this book, namely, the core business systems. These systems are identified herein as procurement, disbursements, payroll, financial statement reporting, inventories, and journal entries.

The auditor needs a methodology (the "M" in ATM) for building a response to detect fraudulent transactions. The fraud response starts in the planning stage with the brainstorming session and continues with the assessment of fraud likelihood and fraud significance. Included in the response are the steps of audit procedures that will reveal the true nature of the transaction (referred to as building a sample of transactions; also known as data mining), implementation of fraud audit procedures, and the final step of evaluating the audit evidence for qualitative and quantitative considerations. These steps are all essential parts of the overall audit response to the fraud risk.

Finally, there is the awareness (the "A" in ATM) required by the fraud audit approach discussed in this book. The auditor needs to be able to recognize fraud scenario potential among the millions of transactions that exist in today's business systems. Knowing the red flags of fraud and recognizing the potential for fraud scenarios inherent to specific organizational structures is critical to the overall process of finding fraud.



WHY RESPOND TO FRAUD RISK?

There are many reasons to detect and uncover fraud. The obvious reasons are the substantial monetary sums and industry-wide and international reputations at stake. There are many studies that have been done projecting the cost of fraud to organizations. The range of results is extreme, with some instances resulting in the cost being minimal to those cases where fraud is found to be so rampant that it causes the destruction of an organization. Organizations like Barring Bank and Enron do not exist today because of the fraudulent actions of their employees. The cost of corruption in public contracts has been estimated to exceed one trillion dollars. Examples abound, too, with large companies still in operation, like the fraudulent allegations regarding numerous Fortune 500 companies. Just pick up a newspaper on any given day and in all likelihood there will be a story concerning fraud. The overriding fact is that fraud costs organizations significant monetary amounts and reputation-harmful publicity each year.

However, organizations do not have to accept fraud as a cost of doing business, and they should not live in a state of denial that their existing internal controls will protect them from fraud. Organizations need to realize that a proactive audit approach is necessary in the detection of fraud. Whether this task is embedded in an internal audit or outsourced to an audit firm is a matter of corporate style and, therefore, should not compromise the overall purpose of finding fraud. Therefore, the primary result of rooting out fraud should be both an increase to the bottom line through financial recoveries and the stopping of future losses.

Professionally, the standards are requiring auditors to respond to the risk of fraud within their audit scope. Consequently, not having a response to fraud is a violation of standards. Other than fear, what is preventing the standards from being followed? As with any standards, regulations, policies, and so on, it comes down to interpretation. What continues to be debated is the breadth of the audit response to the fraud risk. Is a questionnaire sufficient to evaluate fraud propensity? Is the awareness of red flags the right approach? Should auditors search for fraud when no overt internal control red flags are evident? Is a site visit to validate the existence of a customer an audit or investigation procedure? These are all good questions that are being debated in the profession. The answers in all probability will eventually be derived from a combination of three things: the actual attempts at applying the audit standards, customer expectations of the auditors' efforts in finding fraud, and the desire of the auditor to detect fraud.

4 ■ The Fraud Audit

In light of such speculation, this book will focus on the first of these three things, specifically, the techniques that have been tried and proven effective in the detection of fraud. However, given the relevance of the professional audit standards to this discussion, Chapter 2 of this book will provide an overview of the professional audit standards so that the reader can correlate the standards to the processes being discussed.

THE FRAUD PARADIGM

Times have changed. Old problems such as fraud have taken on new attributes because of the technological sophistication of our society. The ease of doing business because of continual technological advances presents opportunities that audit methodologies have not kept up with. We need to think differently about fraud in order to develop a realistic audit approach to fraud risk. There are essential questions that are needed to be asked to close this ever-growing gap.

For example, what is fraud? A simple question, but we still need to be on the same page. As auditors, we need to distinguish the difference between fraud in a legal sense and fraud from an auditor's perspective. We also need to understand the difference between a violation of law and a fraudulent act. From a legal perspective, the act of embezzlement, although a violation of law, is not necessarily a fraudulent act; however, most auditors would consider such an act as fraudulent. Therefore, auditors need a fraud definition that is consistent with the audit process, not the legal system. Words like *fraud scenario*, *intent*, *concealment*, and *damages* should be defined from an audit perspective versus a legal perspective. In order to find fraud, auditors must know what fraud is within the boundaries of the systems they are working in and not those of the law per se.

Should auditors prove fraud? The answer is no. Auditors are not the trier of fact. From a legal perspective, judges and juries are responsible for making the decision. Internally, the decision rests with management or the audit committee, depending on the organization's policies. Auditors are responsible for conducting audits that identify activity that may violate laws or internal policies. The activity should then be referred to the appropriate investigative body. For an analogy, the audit process is like a grand jury. The opinion of the grand jury and the auditor is that sufficient evidence exists to warrant an investigation. Whether the investigation is conducted by the same person is not relevant; however, it is important to note that there is a distinction between the fraud audit process and the legal investigative process.

Can auditors detect inherent fraud schemes within the audit process? Perhaps the answer is not a simple yes or no. Two critical points center on the sophistication of the fraud concealment strategy and the inherent fraud scheme. For example, the revenue-skimming fraud scheme is the diversion of revenue before the revenue transaction is recorded. By the nature of the scheme, there is no record trail. Therefore, the examination of the books and records will not detect the fraud scheme. The sophistication of the concealment is how the individual hides his or her actions, which can be rated as low, medium, and high. If the person uses his home address for his shell corporation, the audit process should be able to detect that scheme. If the individual uses a series of shell corporations using post office boxes, the audit process may not be able to detect the fraud scenario. Understanding what fraud scenarios are detectable within the audit process is critical to planning the fraud audit. Additionally, if the nature of the fraud scenario is not detectable within the audit process, then logically, the organization needs to strengthen internal controls or rely on allegations of the fraud scenario.

Can you have a complex fraud scheme inherent to an organization? No. Most inherent fraud schemes are fairly simple to understand. It is how individuals conceal their actions and shield themselves from the action that may be complex or difficult to detect. Some might say this is a game of words. Maybe so, but the difference between the action and the concealment strategy is an important distinction to know.

FRAUD AUDITING

A fraud audit is the process of responding to the risk of fraud within the context of an audit. It may be conducted as part of an audit, or the entire audit may focus on detecting fraud. It may also be performed because of an allegation or the desire to detect fraudulent activity in core business systems. For our discussion purposes, this book will focus on the detection of fraud when there is no specific allegation of fraud.

Fraud auditing is the application of audit procedures designed to increase the chances of detecting fraud in core business systems. The four steps of the fraud audit process are:

1. **Fraud risk identification.** The process starts with identifying the inherent fraud schemes and customizing the inherent fraud scheme into a fraud scenario. Fraud scenarios in this context will be discussed in Chapter 3.

6 ■ The Fraud Audit

2. **Fraud risk assessment.** Fraud risk assessment is the linking of internal controls to the fraud scenario. The assessment of fraud likelihood is discussed in Chapter 5. Also involved is the use of data mining search routines to determine if transactions exist that are consistent with the fraud scenario data profile. While data mining is highlighted in Chapter 7, it is a relevant part of our discussion throughout the book.
3. **Fraud audit procedure.** The audit procedure focuses on gathering audit evidence that is outside the point of the fraud opportunity. Specific procedures will be discussed in Chapter 8 and have relevance in subsequent chapters.
4. **Fraud conclusion.** The conclusion is an either/or outcome, requiring either referral of the transaction to investigation or the determination that no relevant red flags exist. Chapters 3 through 9 contain relevant discussion of this step.

Traditional Audits versus Fraud Audits

As stated previously, but worth repeating, auditors today have a responsibility to respond to the risk of fraud. What continues to be debated is how to respond to that risk. The discussion centers around the difference between audit procedures performed in a traditional audit versus those performed in a fraud audit. To understand the differences, we first need to define each audit approach, then compare the two. A traditional audit typically focuses on the adequacy and effectiveness of the internal controls. The process is commonly referred to as a test of internal controls. A Generally Accepted Audit Standards (GAAS) audit of the financial statements would also include substantive tests of the financial accounts comprising them. In contrast, a fraud audit is the application of specific audit procedures to increase the likelihood of detecting fraud in core business systems. It is a proactive approach to detecting fraud, unlike a fraud investigation, which takes a reactive approach. The fraud audit does not test controls, but rather independently affirms the authenticity of the transaction by gathering evidence external to the perpetrator.

The two types of audits can also be compared in terms of the differences in sampling methodology, audit procedures, and the qualitative aspects of audit evidence as follows.

The traditional audit requires selecting a sample using random and unbiased sampling procedures in order to opine on the effectiveness of the internal controls. The fraud audit requires selecting a sample using a nonrandom and

bias sampling methodology, based on the fraud data profile, to detect fraudulent transactions. The sampling approach for fraud auditing is commonly referred to as discovery sampling.

In a traditional audit, the audit response is to test controls and examine documentary evidence to verify that the control procedure is operating as designed by management. The resulting conclusion is that controls are or are not operating as management intended. In a fraud audit, the audit response is to perform fraud audit procedures designed to gather evidence independent of company documents. An example can be found by looking at testing in the cash disbursement cycle where the inherent fraud scheme is the use of a fictitious company billing for services not performed. A traditional audit of the cash disbursement cycle relies on the vendor invoice and authorized approval signature. Depending on the controls in place, purchase orders or two levels of approval may be required. The fraud audit does not focus on the controls, but rather on the authenticity of the transaction. In a fraud audit, the auditor will either perform procedures to independently verify if the company exists in the truest business sense or employ a procedure to ensure the vendor is conducting business consistent with that described on the invoice.

Fraud Audit versus Fraud Investigation

The primary distinction between the fraud audit and the fraud investigation is the standards for performing the engagement and the intent of the engagement. The fraud audit is performed under the auditing standards. Whereas fraud investigations are performed using the criminal or civil standards applicable to the jurisdiction, fraud auditing is intended to identify transactions that warrant an investigation. The intent is not to prove fraud, but rather identify the transactions as suspicious. In other words, the transaction has unresolved red flags. The decision tree analysis in Chapter 8 will further elaborate on the concept of a suspicious transaction. Fraud investigation is intended to refute or corroborate the suspicion of fraudulent acts. The law becomes the basis for the methodology and standards. Criminal and civil procedure, rules of evidence, statutes, and burdens of proof are critical element of the investigative process. Even in the fraud investigation, the purpose is not to prove fraud, that obligation is the responsibility of the trier of fact, specifically, either the judge or the jury.

In reality, a fraud audit and a fraud investigation do use many of the same procedures, such as document examination, interviews, and report issuance. In terms of responding to an allegation of fraud, the difference between fraud audit

8 ■ The Fraud Audit

and fraud investigation rests with the eventual Trier of Facts standards. While in regard to the responding to the risk of fraud with no specific allegation of fraud, the difference between audit and investigation seems to balance on the perceived responsibility of the auditor to detect fraud within their audit process.

FRAUD DEFINED

By defining fraud, we hope to establish the scope of the fraud response from an audit perspective. This means that the auditor may adopt the definition as written, or exclude those aspects not relevant to the scope of their audit. However, intent and concealment should never be excluded from the definition. What we are essentially doing in defining fraud from an audit perspective is describing the characteristics of fraudulent acts that differentiate them from similar or like acts. Specifically:

1. Acts committed on the organization or by the organization or for the organization. The first part of the definition focuses on the primary and secondary classifications of fraud, which will be discussed in Chapter 3.
2. Acts committed by an internal or external source. The focus is on the primary party committing the fraudulent act. Obviously, the scenario may include both parties.
3. The acts are intentional and concealed. The intent of the act and how the fraud is concealed differentiate fraud risk from control risk.
4. The acts are typically illegal or denote wrongdoing, such as in the cases of financial misstatement, policy violation, ethical lapse, or a perception issue. The purpose is to distinguish between the illegal act and the act that is not illegal, but conducted with intent and to conceal.
5. The acts cause a loss of company funds, company value, or company reputation, or any unauthorized benefit whether received personally or by others. Fraud by its nature is associated with financial gain.

THE FRAUD TRIANGLE

The fraud triangle explains why people commit fraud. The theory behind it is simple: those with opportunity either rationalize their illicit behavior or are motivated by the pressures to commit the fraudulent behavior. Statement of Auditing Standard 99 requires auditors to understand the fraud risk

factors as part of planning their audit response to the risk of misstatement. Understanding the concept is easy; however, applying the concept in the fraud audit is more of a challenge. The following sections describe the components of the fraud triangle, along with the challenges in the practical application of it.

Opportunity to Commit Fraud

Opportunity is an individual's ability to commit a fraud scenario and his or her related experience in committing the scenario. In the audit planning stage, the fraud opportunity should be viewed absent of any internal controls. The goal is to identify all parties that logically have the opportunity to commit the fraud scenario. The parties can be identified through job title or function; for example, from an internal control perspective, it is a person's job duties that provide an opportunity to commit fraud rather than the level of operation presenting an opportunity to commit fraud. Also, the actual opportunity is either direct or indirect. In Chapter 3 we will further discuss fraud opportunity in context of the permutation analysis.

Opportunity also correlates to one's experience in committing the fraud scenario. We have identified four categories of fraud perpetrators and experience levels as follows:

1. There is the first-time offender, where the pressures and rationalization cause the person to commit the fraudulent act. Remember that opportunity pertains to the ability to commit the fraudulent act and not the cause. There are many theories regarding first-time offenders. Typically, their fraud starts from nothing, as when the perpetrator learns of a control weakness and becomes tempted. Then it grows with each subsequent successful attempt. Consequently, these frauds are usually detected within a few years.
2. The repeat offender is a person who has committed a fraud scenario in more than one organization or committed fraudulent acts numerous times, but in different areas of the company without detection each time. This description indicates that opportunity is the critical factor involved with the intent to commit fraud a multiple of times, with the causes of pressures and rationalization being less significant factors.
3. The organized crime category pertains to a group of people external to the organization who are dedicated to committing the fraudulent act. Again, pressures and rationalization are not as critical as is opportunity. Often,

10 ■ The Fraud Audit

individuals in this category will extort or bribe employees to participate in the fraudulent act, or members of the organized crime group will seek employment within the organization to commit the act.

4. For the benefit of the company category, the individuals involved typically see their action as benefiting the organization; therefore, rationalization is typically the cause. These individuals are characteristically high-ranking employees in the organization. While they benefit from their actions as individuals, they also believe their actions are for the good of the organization.

Knowing these categories is useful in understanding how the fraud triangle theory correlates to the tendency for committing fraud. Also, they highlight why internal controls sometimes fail to stop a motivated person from committing the fraudulent activity. Within the fraud audit, the opportunity to commit fraud is the critical consideration, as seen with the experience factors just described. For example, the control owner has the primary opportunity to commit the fraud scenario. Consequently, linking the inherent fraud scheme to the person with the opportunity becomes the basis for identifying the fraud scenarios related to a particular business system. Using the fraud permutation analysis will also bring to light other fraud opportunities that are not considered in a more traditional, control-based audit. Clearly, understanding the fraud opportunities and linking them to an inherent fraud scheme is a critical first step before an audit response can be planned and executed.

Pressures Affecting People or Organizations

The identification of pressures will vary with the nature of the primary classification of fraud. Typically, the pressure is associated with financial reasons. For example, pressures are evident in financial reporting's meeting investors' expectations of more income, leading to asset misappropriations, a primary fraud classification. The key is to understand which pressures correlate to which primary fraud classification, but more on that in Chapter 3. For now, you have to know that an audit, by its nature, generally does not have procedures to accurately gather information that would disclose these issues with any certainty. However, the audit process can create an awareness of behaviors in the workplace indicative of a lifestyle-maintenance issue creating pressure. It is interesting to note that in a subsequent investigation, private investigators would collect information to be used regarding behaviors that relate to vices or other lifestyle anomalies.

Rationalization of Fraudulent Behavior

People rationalize their behaviors. The reasons vary from person to person, but a justification always exists. Fundamentally, rationalization is a conscious decision by the perpetrator to place his or her needs above the needs of others. Even though the ethical decision-making process varies by individual, culture, and experience, rationalization is present. The concept is important in the understanding of why people commit fraud. You can put two employees in the same job duties with the same opportunity to commit fraud. One will take the opportunity and the other will not. How the one who does take the opportunity rationalizes the fraud speaks to the cause and not the opportunity. Therefore, when you think of the practicality of using the rationalization concept to identify fraud, you are limited to being observant to lifestyle behaviors.

Fear of Detection

The reasons for not committing fraud are numerous. Personal integrity, family values, and religious beliefs are just a few of them. One reason, outside the area of virtues, morals, and character, is the fear of detection. There we go talking about fear again, but the fear of being detected is a very significant factor in discussing fraudulent behavior. From an internal control perspective, once pressure and rationalization exceed the fear of detection, people are more prone to committing a fraudulent act. This condition is important to understand, especially when auditors place too much reliance on an internal control's ability to mitigate a fraud risk. This does not mean that internal controls are to be ignored. They are one of the important defenses in preventing fraud. However, in assessing the likelihood of fraud, the fear of detection, or the lack thereof, is an intangible; that is, it is difficult to assess, and therefore is not a part of our discussion of factors mitigating risk in a fraud audit.

Fraud Triangle Premises

The body of knowledge surrounding the fraud triangle is critical to the fraud auditor. The ATM approach to a fraud audit relies on the concepts denoted by the fraud triangle. The triangle as a whole is critical in the planning phase for the recognition of the tendency for fraud within the core business system. In particular, designing the methodology for the data mining, audit procedures, and evidence considerations relies on the fraud opportunity. The following summarizes key considerations regarding the fraud triangle:

12 ■ The Fraud Audit

1. The three elements of fraud—rationalization, pressure, and opportunity—coexist at different levels per individual.
2. The three elements of fraud will vary based on personal circumstances of the individual.
3. The strength of one element may cause an individual to commit a fraudulent act.
4. The strength of one element may eliminate the worry of fraud detection.
5. Identifying the three elements is easier than measuring the three elements.
6. The fraud risk factors may originate from internal or external sources.
7. Fraud opportunity is the one aspect of the fraud triangle that is easily identifiable.
8. The fraud audit is based on the opportunity to commit an inherent fraud scheme.

RESPONSES TO THE RISK OF FRAUD

There are two fundamental approaches to responding to the risk of fraud. The first approach is to test internal controls and be alert to the red flags of fraud. The second approach is to actively search for the existence of fraud scenarios that are occurring in the core business systems and not rely on internal controls. The approach used is dependent on the purpose of the audit and the applicable audit standards.

The methodology for responding to the risk of fraud will vary depending on the professional standards and the purpose of the audit, that is, financial statement audits will apply Generally Accepted Audit Standards. In particular, Statement of Auditing Standards 99 provides guidance to responding to fraud risk in a financial statement audit. The overall purposes can be categorized in the following four groups:

1. Reliance on internal controls for purposes of a financial statement audit. In the financial statement audit, the auditor will test internal controls and be alert to the red flags.
2. Provide an opinion on the operating effectiveness of the internal controls regarding fraud minimization. The internal controls are tested and alert to the red flags.
3. Provide an opinion on the existence of fraud in core business systems. In the fraud audit, the auditor does not rely on internal controls and instead actively searches for fraud. The internal controls are considered to

control avoidance strategies, circumvention strategies, and inhibitor considerations.

4. Respond to an allegation of fraud. The investigation by design is intended to refute or corroborate the allegations. The existence or avoidance of internal controls may be relevant to establishing intent.

The types of methodologies to responding to the risk of fraud are the following:

1. **Red flag approach.** The purpose is to test the effectiveness of internal controls and be alert to the red flags that are consistent with the fraud scenario. In a financial statement audit, the purpose is to determine the reliance on internal controls as part of the decision process on substantive testing procedures. Internal auditors test internal controls to determine the effectiveness of the internal control. Understanding the red flags is critical to both the awareness and the methodology of the fraud response.
2. **Integrate a fraud audit procedure into an audit program.** The purpose is to respond to a specific fraud scenario. Does the identified fraud scenario result from a perceived risk within the risk assessment or a mandatory fraud risk such as revenue recognition as required by SAS 99?
3. **Fraud audit.** The purpose of the fraud audit is to uncover fraud in the core business systems and be alert to internal control weaknesses regarding fraud opportunity.
4. **Fraud allegation response.** The purpose is to refute or corroborate the allegation of fraudulent activity

SUMMARY

Although the methodology for conducting a fraud audit is different from traditional auditing, the auditor employs many of the same skills and tools. Therefore, fraud audits are a blend of new methodologies and traditional audit tools. Instead of debating whether the procedure is a traditional audit, fraud audit, or fraud investigation, this book will direct its efforts toward what the auditor can do to uncover fraud in the places it is most often found: the core business systems.

