1

Fraud Theory

Auditors today are at a crossroads regarding how to incorporate fraud detection into their audit plans. Sarbanes-Oxley, Public Company Accounting Oversight Board (PCAOB) regulators, and the professional standards of auditing are requiring auditors to give greater consideration to incorporating fraud detection into their audit plan. Companies' boards of directors, management, and the public are asking why is fraud occurring and going undetected in our business systems. Auditors are asking themselves whether fraud can be detected when there is no predication or allegation of a specific fraud.

Traditionally, the auditing profession had two fundamental ways to deal with the fraud question:

1. Search for fraud using a passive approach of testing internal controls. The approach relies on auditors seeing the red flags of fraud. Although few audit programs incorporate specific red flags for audit observation, the assumption is that professional experience will provide auditors with the skills to observe the red flags.
2. React to fraud allegations received through a tip or some other audit source. Since studies continue to indicate that most frauds are detected through tips, we need to ask ourselves how effective past audit approaches have been.

Historically, the profession relied on evaluating the adequacy and effectiveness of internal controls to detect and deter fraud. Auditors would first document the system of internal controls. If internal controls were deemed adequate, the auditors would then test those controls to ensure they were operating as intended by management. The test of internal controls was based on testing a random, unbiased sample of transactions in the business system. Conventionally, audit standards stated that auditors should be alert to the red flags of fraud in the conduct of an audit. Study after study indicates that the lack of professional skepticism is a leading cause for audit failure in detecting fraud.

In one sense, the search for fraud seems like a daunting responsibility. However, fraud in its simplest form should be easy to find. After all, the key to finding fraud is looking where fraud is and has been. This book focuses on the use of fraud auditing to detect fraud in core business systems. Fraud auditing is a proactive audit approach designed to respond to the risk of fraud. Essentially, the fraud audit approach requires auditors to answer these questions:

- Who commits fraud, and how?
- What type of fraud are we looking for?
- Should fraud be viewed as an inherent risk?
- What is the relationship between internal controls and fraud opportunity?
- How is fraud concealed?
- How can we incorporate the fraud theory into our audit approach?
- What are the ways fraud auditing can be used to detect fraud?

BUILDING FRAUD THEORY INTO THE AUDIT PROCESS

Fraud auditing is similar to, but different from traditional auditing in several ways. Typically, an audit starts with an audit plan, whereby, risks are identified through a risk assessment, controls are linked to the risks, sampling plans and audit procedures are developed to address the risk(s) identified. The audit steps are the same regardless of the system(s) being targeted. Throughout the process, the auditor must have an understanding of the system(s) being audited. For example, to audit financial statements, auditors must understand generally accepted accounting principles (GAAP). In the same way, to audit a computer system, auditors must understand information technology (IT) concepts.

Using the Fraud Risk Assessment

If the steps are the same, then what feature makes fraud auditing different from traditional auditing? Simply, the body of knowledge associated with fraud. The fraud theory must be built into the audit process. Specifically, during the audit planning stage, auditors must determine the type and the size of the fraud risk. By performing a fraud risk assessment, the identified fraud risk is associated with the core business systems. As in the traditional audit, controls are linked to the risk, but in this circumstance it is the fraud risk that is targeted. By incorporating the fraud theory in the fraud risk assessment, the concealment strategies employed by the perpetrator(s) are also considered. Auditors rely on the red flags of fraud to prompt awareness of a possible fraudulent event, known as the specific fraud scheme. The sampling plan is used to search for the transaction indicative of the specific fraud scheme. Then, the audit procedure is designed to reveal the true nature of the transaction.

The Principles of Fraud Theory

Although the fraud risk assessment is a practical tool, there are principles upon which fraud auditing is based that auditors should know before initiating a fraud audit plan. These principles are as follows:

- Fraud theory is a body of knowledge.
- Fraud is predictable to the extent of how it will occur in a specific situation, not necessarily in the actual occurrence.
- The key to locating fraud is to look where fraud occurs.
- If you want to recognize fraud, you need to know what fraud looks like.
- People commit fraud, not internal controls.
- Fraud risk and control risk have similarities. However, fraud risk differs from control risk by containing the elements of intent and concealment.
- Fraud audit procedures must be designed to pierce the concealment strategies associated with the fraud scheme.
- Fraud audit procedures must validate the true economic substance of the transaction.
- Fraud audit comments differ from the traditional management letter or internal audit report.

ATM: AWARENESS, THEORY, METHODOLOGY

Fraud is like an ATM machine at a bank. Both are designed to withdraw money. ATM machines enable users to withdraw money from banks. Fraud is the withdrawal of funds from an organization. The funds may be embezzled directly, siphoned off through kickback schemes, or be the result of inflated costs due to bribery and conflict of interests. The fraud audit approach requires awareness, theory, and methodology (ATM) to detect fraud. Successful auditors need:

Awareness of the red flags of fraud:

- Fraud concealment strategies
- Sophistication of the concealment strategy
- Indicators of fraudulent transactions

Theory provides an understanding how fraud occurs in a business environment:

- Fraud definitions
- The fraud triangle

Methodology designed to locate and reveal fraudulent transactions. The methodology employed in designing a fraud audit program consists of the following stages:

- Define the scope of fraud to be included and excluded from the audit program.
- Verify compliance with the applicable professional standards.
- Develop the fraud risk assessment including:
    - Identify the type of fraud risk.
    - Identify business processes or accounts at risk.
    - Internal controls are linked to the fraud risk.
    - Concealment strategies revealed using the red flags of fraud.
    - Develop a sampling plan to search for the specific fraud scheme.
    - Develop the appropriate fraud audit procedures.
- Write the fraud audit report.
- Understand the fraud conversion cycle.
- Perform the fraud investigation.

The search for fraud is built on both awareness and methodology; however, both items are predicated on auditors having a sufficient knowledge of the science of fraud, hence the fraud theory. Auditors are not born understanding fraud. The awareness needs to be incorporated into the audit plan through audit team discussions during the planning stages. Audit programs must incorporate a methodology that responds to the identified fraud risks existing in core business systems.

Theory

The "T" in ATM stands for theory, specifically, fraud theory. Given that the knowledge of fraud theory is needed by auditors in order for "awareness" to be incorporated into the audit plan and for a "methodology" to be established, the specific elements of fraud theory need to be discussed as a first step.

Definitions Inherent to the process of searching for fraud is having a clear definition of fraud to be incorporated into the fraud risk assessment. Throughout the process, a thorough understanding of the fraud theory is critical to an auditor's success in preventing, detecting, deterring, and prosecuting fraud.

Auditors need to understand that fraud is an intentional and deliberate effort by the perpetrator to conceal the true nature of the business transaction. Fraud perpetrators have varying levels of sophistication, opportunity, motives, and skills to commit fraud.

The fraud risk assessment starts with a definition of fraud and the type of fraud facing organizations. The assessment can be based on a legal definition, an accounting definition, or the author's definition specifically designed for fraud risk assessments.

The Legal Definition

- A known misrepresentation of the truth or the concealment of a material fact to induce another to act to their detriment.
- A misrepresentation made recklessly without the belief in its truth to induce another person to act.
- A tort arising from a knowing misrepresentation, concealment of material fact, or reckless misrepresentation made to induce another to act to their detriment.
- Unconscionable dealing especially in contract law. The unfair use of power arising out of the parties' relative positions and resulting in an unconscionable bargain.

The legal definition requires auditors to understand the legal implications of the terms in the definition. The term "misrepresentation" includes concealment, nondisclosure, or false representation. The misrepresentation must relate to a material fact rather than a simple opinion. However, opinions made by an individual purportedly with superior knowledge could become a misrepresentation. Concealment, referred to as suppression of facts, is also a critical aspect of the misrepresentation. The courts have accepted these theories of concealment:

- Intentional concealment of known defects.
- Active prevention of the discovery of the defects.

- Uttering lies, with the intent to deceive.
- Nondisclosure typically does not rise to the level of fraud, unless a fiduciary relationship exists.

In reality, the use of the legal definition of fraud is impractical for most audit organizations simply because the definition is written for civil and criminal prosecutions.

The Accounting Definition Given the specific usage of the legal definition, auditors typically look to the applicable professional standards followed by the audit organization. The American Institute of Certified Public Accountants (AICPA) offers guidance in its Statement of Auditing Standards (SAS No. 99) as to the auditor's responsibilities to detect fraud that would have a material impact on the financial statements. The standards focus on financial statement and asset misappropriation schemes. Interestingly, the standard does not provide a definition of fraud. Rather auditors are guided by the standard definitions of errors in financial statements. An example of a professional standard applicable to fraud is the Institute of Internal Auditors Standard 1210.A2.

The Institute provides guidance on *Auditor's Responsibilities Relating to Fraud Risk Assessment, Prevention, and Detection*. The standard states that internal auditors should have sufficient knowledge to identify the indicators of fraud, but they are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud. The standard contains a section called "What is Fraud." This section states:

Fraud encompasses a range of irregularities and illegal acts characterized by intentional deception or misrepresentation, which an individual knows to be false or does not believe to be true. Throughout this practice advisory, and in PA1210.A.2-2, the guidance may refer to certain actions as "fraud," which may also be legally defined and/or commonly known as corruption. Fraud is perpetrated by a person knowing that it could result in some unauthorized benefit to him or her, to the organization, or to another person, and can be perpetrated by persons outside and inside the organization.

The institute provides guidance on auditor's Practice Advisory 1210. A2-2: *Auditor's Responsibilities Relating to Fraud Investigation, Reporting, Resolution and Communication.*

The Author's Definition of Fraud Acts committed on the organization or by the organization or for the organization. The acts are committed by an internal or external source and are intentional and concealed. 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 acts cause a loss of company funds, company value, or company reputation, or any unauthorized benefit whether received personally or by others.

The Fraud Triangle Once a fraud definition has been adopted, the fraud triangle must be incorporated into the fraud audit plan. Therefore, fraud theory includes an understanding the fraud triangle.

The fraud triangle is generally accepted as part of the process of identifying and assessing fraud risk. The concepts are inherently simple. The fraud theory states that for fraud to occur there needs to be rationalization, pressure, and opportunity. The AICPA has referred to these three elements as the fraud risk factors or conditions of fraud.

Rationalization People rationalize. The reasons vary, but the justification always exists. Fundamentally, rationalization is a conscious decision by the perpetrator to place their needs above the needs of others. The ethical decision process varies by individual, culture, and experience. The ability to identify and rank rationalization is difficult on a person-by-person basis within the audit process, because of the fact that organizations are comprised of a number of individuals. Therefore, at an organizational or departmental level, the issues influencing individuals are easier to determine.

Pressures The pressures are the events occurring within the organization or in the individual's life. The pressures vary by the global risk factor. With the

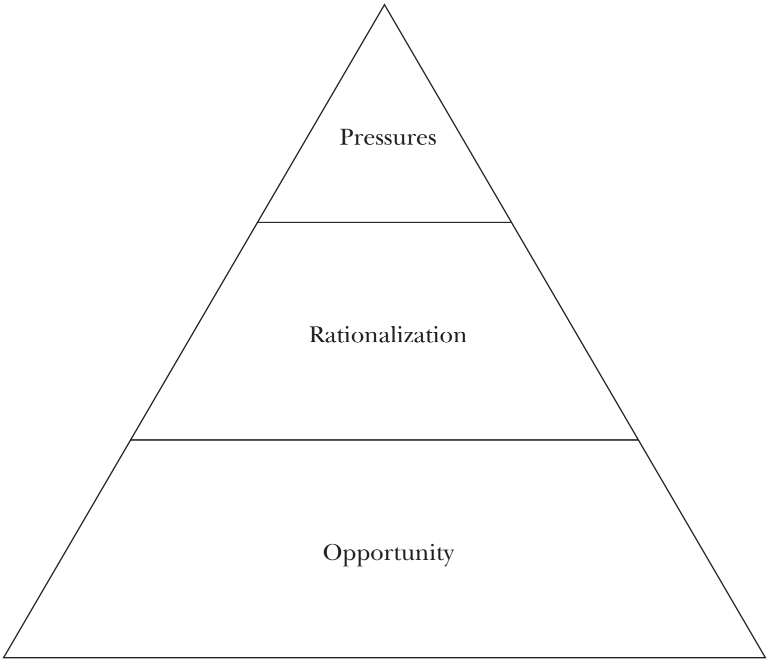

Exhibit 1.1 The Fraud Triangle

pressures of fraud, the individual's personal needs become more important than personal ethics or the organization's needs and goals.

The motive to commit the fraud is often associated with personal pressures and/or corporate pressures on the individual. However, the motive is actually the willful desire to commit the fraudulent act. The motive to commit fraud may be driven by the pressures influencing the individual, by rationalization, or by sheer opportunity.

Opportunity To commit a fraud, an individual must have access to the asset or manage a control procedure that allows the commission of the fraud scheme. A person's position, as well as, their responsibilities and authorization, also contribute to the opportunity to commit fraud. There is a direct correlation between opportunity to commit fraud and the ability to conceal the fraud. In assessing the fraud risk factor, auditors need to consider both opportunity and the ability to conceal in the design of an audit plan.

Premises Six premises must be understood in applying the fraud triangle concepts:

1. The three elements of fraud—rationalization, pressure, and opportunity—coexist at different levels per individual.
2. The elements of fraud will vary based on personal circumstances.
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 detection.
5. Identifying the three elements is easier than measuring the three elements.
6. The fraud risk factors may originate from internal sources or external sources.

The three elements of fraud coexist at different levels within the organization and influence each individual differently. The strength of one element may cause fraud to occur or some combination of the elements. Perhaps the strength of an element may eliminate the perpetrator's fear of detection. Therefore, the fraud assessment process must consider the fraud conditions.

Measuring the three elements of the fraud triangle is not as simple as taking someone's temperature. The audit process should identify and understand how the fraud conditions lead to the likelihood of fraud. In reality, identifying the fraud condition is easier than measuring the elements. The audit process should be aware of the fraud condition, but ranking the three factors is highly subjective.

Methodology

Methodology addresses the scope of the fraud audit and the subsequent design of the fraud risk assessment. The primary purpose of the fraud risk assessment is to identify the risks of fraud facing an organization. The assessment process evaluates the likelihood of fraud occurring and the extent of exposure to the organization if the fraud event occurs. Such an assessment can be used at various levels of an organization, such as, at the enterprise-wide level or at the business process level. Regardless of level, the assessment methodology must classify the fraud schemes by organizational function. Then a specific fraud scenario can be ascertained for each fraud scheme possible in the organization.

For example, to develop an enterprise-wide fraud risk assessment, the following steps are performed:

1. Create an enterprise-wide category of fraud.
2. Identify the type of fraud that associates with the enterprise-wide category of fraud.
3. Target the major operating units of the organization, for example, company subsidiaries or departments.
4. Target major business systems or accounts in the operating unit, for example, revenue or procurement.
5. Identify the inherent fraud schemes that link to a specific account or business system.
6. Determine the variation of the inherent fraud schemes. This occurs at the business process level.
7. The variation of the fraud scheme is linked to the opportunity to commit the fraud. This is referred to as the fraud scenario.

Fraud Schemes Through a fraud scheme or “identified fraud risk,” a fraud is perpetrated and concealed in a business system such as: account balance, class of transactions, or presentation and disclosure assertions. The fundamental mechanics of fraud schemes are the same for each organization, but how a scheme occurs within each organization may differ. Due to the differences, the identified fraud risks should be considered as an inherent risk. Therefore, in developing the list of fraud schemes for the core business systems, remember these basic tenets:

- Each core business system has a finite list of inherent fraud schemes.
- Each fraud scheme is perpetrated by an individual. This action is referred to as fraud opportunity.

- Each fraud scheme may have a series of variations.
- Each fraud scheme variation has various fraud scenarios.
- Each fraud scheme occurs differently in each industry and each company or organization.
- Each perpetrator is confident that they will not be detected.
- Each fraud scheme has a unique concealment strategy and characteristics.
- Each concealment strategy has associated red flags.
- Each fraud scheme has a unique data profile.
- The objective of each fraud scheme is the initiation of the conversion cycle in which the perpetrator converts the fraud scheme to personal gain.

Inherent Fraud Schemes The fraud risk assessment process starts with identifying the fundamental fraud scheme, also known as the inherent fraud risk schemes, facing an organization and/or a specific business system. Later chapters will list and describe the inherent fraud schemes.

The Fraud Circle The fraud circle illustrates the relationship between fraud theory, as discussed in this chapter, with the concept of fraud response and

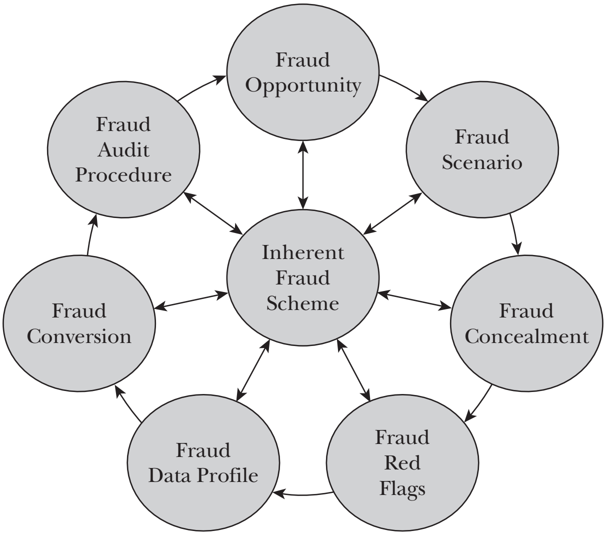

Exhibit 1.2 The Fraud Circle Chart

the fraud audit, as discussed in Chapter 2. Exhibit 1.2 shows how an inherent fraud scheme may be linked to an appropriate fraud response.

Fraud Opportunity Considerations A person's position in terms of their responsibilities and authority also contribute to the opportunity to commit fraud. The fraud opportunity phase starts with a list of the fraud schemes that individuals can commit by the virtue of their position within the organization. It should be noted that breakdowns in control procedures also create fraud opportunity referred to as internal control inhibitors.

In today's business environment, internal controls do not always function as intended by management. While the business transaction may indicate that the control is functioning, the employee is not performing the control procedure with the control guidelines. The nonperformance of an internal control negates the control's effectiveness. This problem is referred to as the control reality versus control theory.

Fraud occurs because individuals use their positions to intentionally override controls. This override can occur at any level having access to the control, for example, the employee level, the supervisor level, or the senior management level. The override occurs by one person or in collusion with other employees.

In addition, fraud risk assessments should consider logical collusion. Many fraud schemes by their nature can only be committed with such collusion. For example, bribery and corruption schemes occur because of collusion between a vendor or customer, and an employee. Over time, fraud often involves collusion between supervisors and employees. The occurrence of logical collusion does not mean that auditors should consider every possible combination of collusion; nor should auditors ignore the fraud schemes that necessitate collusion.

Fraud may simply occur when no control has been established. This oversight results in management's failure to identify a fraud risk opportunity that allows a fraud scheme to operate undetected.

Understanding the opportunity for fraud to occur allows auditors to identify, which fraud schemes an individual can commit, and how fraud risks occur when the controls do not operate as intended by management. Auditors should also consider the sophistication of the individual committing fraud. One approach to profile individuals is to understand the experience they have in committing the fraud and what motivates them to do so.

Perpetrators of fraud against an organization can be classified into four groups:

1. **First-time offenders.** These individuals have no record of criminal activity. They have either a pressure in their lives that exceeds their income capacity or their rationalized behavior indicates that it is fine to embezzle. Once the pressure or rationalization factor exceeds

the fear of detection, the individuals look for the internal control weakness or the opportunity to commit fraud.

2. **Repeat offenders.** Crime statistics have indicated that people who commit internal fraud have a high tendency to commit the crime more than once. In these instances, the pressure and rationalization aspect of the theory will be less dominant than with the first-time offender. Opportunity becomes the driving force to commit the fraud.
3. **Organized crime groups.** These groups consist of fraud professionals who are external to the organization. The groups may be organized professionally or may be groups of individuals who specialize in a particular type of crime. The key factor is the opportunity to commit the crime. These groups may commit crimes by taking advantage of weak internal controls, bribing or extorting employees, or through collusion with vendors or customers.
4. **Internally committed for the perceived benefit of the corporation.** These crimes are usually committed by employees who believe the act is for the good of the company. Typically, pressures and rationalization for these employees are similar to those of the first-time offender or the repeat offender.

Understanding the individual's crime experience and motivation is a key ingredient to preventing and detecting fraud. The fear of detection is often viewed by management as a deterrent to committing fraud. Once the pressure or rationalization exceeds a certain level, the individual fears the pressure or rationalization more than the fear of detection. The opportunity may also be so persuasive for the perpetrator, that the fear of detection seems remote.

Fraud Scheme Scenario A fraud risk assessment always begins with the identification of the fundamental fraud scheme, also referred to as the inherent fraud risk. Once identified, the fundamental fraud scheme can be dissected into the variations applicable to the organization and/or its business systems. Once the variation or variations are isolated via control analysis, a fraud scheme scenario can be ascertained. The fraud scheme scenario should describe how the scheme occurs within the organization and/or its business process. The description should identify the opportunity for the fraud to occur and the methods used to conceal the fraud. The scenario could also describe the fraud conversion strategy, in essence, describing how the scheme would occur within the company and the specific business process.

Fraud Variations

Entity and Transaction Variations Each inherent fraud risk may have several variations. The design of the fraud data mining and/or the fraud audit procedure is dependent on the specific fraud scheme variation.

When analyzing fraud variations, two aspects should be considered: entity variations and transaction variations.

The entity variation analysis identifies how the vendor, customer, or employee would be established or created to provide the appearance of a legitimate source of the fraudulent activity. The transaction analysis identifies variations of how the transaction is processed and recorded due to organizational size, geographic location, management operating style, or nature of the transaction. The variations occur either intentionally or naturally.

The variation analysis should also consider the opportunity to commit the act. At the initial assessment, auditors should identify person responsible for the control procedure and how duties are separated to establish the control environment. The second phase is to consider a logical override or logical collusion by the person responsible for the control procedure.

Industry Variation Industry fraud variation is defined as the process of converting the inherent fraud risk to a specific risk associated with the industry. By understanding how the fraud risk occurs, auditors can better develop a sampling strategy and a specific audit response for the fraud scheme. How fraud schemes operate in each industry varies by the nature of the industry and the organization. For example, revenue skimming, the diversion of a revenue stream before the transaction is recorded is an inherent fraud risk. Therefore, how the scheme occurs and is concealed in any one industry will vary, but the inherent scheme is still the same.

Awareness

Earlier it was stated that the fraud audit approach requires awareness, theory, and methodology (ATM) to detect fraud. To be successful, auditors need to be especially aware of the red flags of fraud. To comprehend how the red flags of fraud are incorporated into the fraud risk assessment, one must first understand fraud concealment strategies and fraud conversion, both acts performed by the perpetrator(s).

The Red Flags of Fraud The "red flag of fraud" is a common term associated with fraud identification. The red flag indicates that there is a potential for a fraud scheme. However, it does not necessarily indicate a fraud scenario has occurred. Observing a red flag is the triggering event for a fraud audit. The term red flag is associated with a specific concealment strategy. The perpetrator uses the concealment strategy to hide the fraudulent transaction. The auditor uncovers the fraudulent transaction by observing a red flag event. Red flags can be categorized by control opportunity, fraud data profile or the documentation. Not all red flags have the same weight or value. However, the weight of the red flag or the total number of red flags does correlate with the likelihood of a fraudulent transaction.

Fraud Data Profile What does a fraudulent transaction look like? In general, the transaction looks like every other one. The fact of the matter is specific data profiles are associated with specific fraud scenarios. When auditors create a fraud data profile, they use data to identify fraudulent transactions within the population of transactions known to a company business system. The data profile will be unique to each specific fraud scheme. In reality, our ability to identity the data profile of a fraud scheme varies by its nature.

Data Mining Data mining is the process of searching for a transaction that meets the fraud data profile. In essence, when searching for fraud, auditors develop a sampling plan that is focused and biased toward a specific fraud scheme. This sampling, performed as a part of the fraud risk assessment, is referred to as data mining because of the particular transactions being sought.

Fraud Concealment A key element of the fraud risk assessment concerns concealment strategies employed by the perpetrator(s). The auditors must understand the confidence factor of the perpetrator and concealment strategies associated with the fraud scheme.

The Confidence Factor Committing a fraud presents the need to conceal the activity. The individual committing the fraud has to have the confidence that the fraud will not be detected. There is a direct correlation between concealment and confidence. If the individual is not confident the act can be concealed, they are not likely to commit the fraud unless the pressures or rationalization factors are so high that the person's logic is overcome.

The Concealment Strategies When individuals decide to commit internal fraud, a critical aspect of their plan is how to conceal the true nature of the transaction. The goal of perpetrators is to have the business transaction look like a properly approved transaction. Characteristically, each fraud scheme has a method of concealment. However, how individual implements the concealment strategy varies, based on the person's position vis-à-vis opportunity and the company's internal procedures.

The sophistication of the fraud scheme varies with perpetrator. In the simplest strategy, the perpetrator assumes that no one is looking or that the sheer size of the transaction population will hide the fraudulent transaction. An example of a complex strategy would be the use of multiple front companies, which involves management override and off-book bank accounts worldwide.

Methods to conceal the true nature of the transaction will vary with the business system, employee position, the use of computerized systems versus manual systems, required documents, internal controls, and corporate governance issues. In some instances, an individual may use more than one layer of concealment techniques to hide the true nature of the business transaction.

Usually the weak point of the fraud scheme is how the perpetrator conceals the true nature of the transaction. If an auditor can identify the concealment strategy of the fraud and question the transaction, the fraud typically will become apparent. The auditor should also be able to recognize the difference between a generic and a business specific concealment strategy. For example, in the overbilling fraud scheme an inadequate product description is a generic concealment strategy. To identify the related business specific concealment strategy, the auditor must be able to recognize a complete and accurate product description on the vendor's invoice. Generic concealment strategies include:

- Management override. An employee uses their position of authority to approve a transaction or encourage other employees to approve the transaction.
- Collusion. Collusion allows employees to circumvent the control procedures. The employees performing the control procedure provide the illusion that the control is operating. In essence, they provide a false representation of the transaction.
- Blocking the flow of information. This can occur in many ways:
    - Layering a transaction. The transaction has to be processed by multiple individuals or entities so no one individual has the full picture.
    - Use of intermediaries.
    - Labeling the transaction as confidential.
    - Using secrecy standards.
    - Using people in a position of trust to provide legitimacy.
- Cross-border/geographic distance. Creating a physical distance between the control functions and the location of the documents.
- Direct pressure on manager. The manager is either bribed or extorted to approve a transaction.
- Direct pressure based on the person's relationship with the company. A vendor or a customer causes a company manager to approve a transaction.
- Processing a transaction below the "control radar." The dollar value, nature of the transaction, or management interest is below the control threshold.
- False documentation. False documentation may include an altered, missing, or created document. A professional perpetrator may use advanced techniques that require a forensic document expert to reveal the false document.

- Changes to internal controls or audit trails. These changes diminish the ability to place responsibility for an error.
- Complexity of the transaction. The lack of understanding would diminish the auditor's ability to recognize the concealment strategy.
- Concealing transactions among other transactions. Here the sheer number of transactions enables fraudulent ones to be concealed.

Fraud Conversion

Fraud conversion is the process of converting the fraudulent act to an economic gain for the perpetrator of the act. In essence, it is the money trail. The aim of the fraud audit is to identify a suspicious transaction that warrants an investigation. The investigation gathers evidence that an illegal act has occurred. Depending on the burden of proof required by law, one element of the investigation is to show that the individual received financial gain from the fraudulent act.

Auditors should be aware of the various conversion techniques in order to avoid reaching a false conclusion during the audit process. Typical conversion strategies are:

Theft of Company Funds

- Theft of cash/currency
- Check theft and false endorsement or check alteration
- Counterfeiting of company checks
- Unauthorized charges on company credit cards
- Wire transfers to unauthorized accounts

Embezzlement of company funds:

- Incoming checks negotiated through a look-alike bank account name or false endorsement
- Company check issued to shell company bank account
- Company check issued on other false pretense or disguised purpose

Kickbacks

- Economic gratuities from vendor or customer/goodwill offerings
- Vendor provides goods or services
- Hidden ownership in vendor or customer
- Hiring family or related parties

Asset Conversion

- Sale of company asset
- Theft of asset
- Personal use of an asset without theft
- Use of apartments, boats, or airplanes
- Purchase of asset below fair market value (FMV)

Disguised Third-Party Payments

- Prepaid credit cards and telephone cards
- Gifts
- Event tickets
- Entertainment and travel

Disguised Compensation

- Conflict of interest
- Disguised compensation
- Disguised fringe benefit
- Stock options manipulation
- Undisclosed loans
- Acquisition of asset below FMV
- Misuse of company assets
- Disguised real estate leases

THE FRAUD AUDIT

There are three approaches to a fraud audit: the passive approach, the reactive approach, and the proactive approach. The proactive approach is known herein as the fraud audit approach. Auditors taking this approach are searching for fraud when there is no fraud alleged or there are no control weaknesses indicating fraud occurring. The fraud audit approach can be utilized as an overall response to the risk of fraud. The fraud audit itself is the application of audit procedures to a population of business transactions in a manner to increase the propensity of identifying fraud. These concepts will be discussed in Chapter 2.

Global Risk

Chapter 3 discusses the fraud risk assessment. Specifically, analysis of the purpose of a fraud audit risk assessment from both an enterprise-wide and a business process view.

The Fraud Risk Audit Program

Chapter 4 discusses the fraud risk audit program as it pertains to fraud risk at the mega-risk level. The tool used is the fraud penetration assessment rather than the enterprise-wide risk assessment or the business process risk assessment.