Demystifying Fraud

LEONARD W. VONA

Leonard W. Vona

DEMYSTIFYING FRAUD

Fraud is not predictable as to when it will occur but it is fairly straight forward as to how it will occur.

Fraud is not predictable as to when it will occur, but it is fairly straight forward as to how it will occur. This is one of the main tenants we like to employ at Fraud Auditing Inc., in order to better detect and prevent fraud. While fraud itself is never completely unavoidable for an organization, knowing the various permutations of how one fraud scheme can occur can give your teams the upper hand when it comes to improving their audit processes.

It can often feel like an impossible task to amalgamate methodology into a cohesive strategy when it comes to fraud — understanding how approaches can be practically applied is key for many audit teams when fraud isn't something they've had to deal with on a day-to-day basis. This eBook will place fraud-based approach methodology into context using worked examples. It will do this by examining the audit approach in a new light, using a fraud-based approach to prevention and detection, as well different kinds of fraud schemes encountered by auditing teams. I have also illustrated different schemes with varying levels of complexity.

While this eBook is not intended to serve as a definitive guide to fraud, it should better assist your approach and ensure that when fraud does occur your teams have the tools to detect and prevent, schemes where possible. By the end of this eBook you should have a fairly robust understanding of common fraud schemes, fraud risk statement (also known as fraud scenario or fraud risk assessment) creation, and using fraud risk detection procedures as part of your approach to uncovering fraud in core business systems.

Common Fraud Schemes

Knowing where and how fraud occurs can be a crucial step towards improving your fraud detection and prevention procedures, saving your client or your company a significant amount of money and time. Here are common fraud schemes.

Shell Company Schemes

Shell company schemes use a fake entity created by an employee to charge their company for a service or product it never receives. The money from this payment ends up in the employee's pocket. This fake entity is legally created but often has no active business per se.

The purpose of this scheme is to conceal the real identity of the company or employee fraudulently acquiring funds through the shell company. The shell company only truly exists on paper although with more sophisticated fraud concealment strategies fraudsters may create an office or hire employees to create the illusion of legitimate business.

Forming a shell company is easy. Although submitting the necessary filings to register a company in the states includes items such as a company name, a name and address of agent for service of process and signatures of incorporators these are generally not verified before the state accepts formation. In some cases, in a matter of minutes you have yourself a shell company.

A more complex shell company scheme is the pass-through scheme. The scheme provides the illusion of an arm's length business transaction with a real company. The goods and services are received, the internal three-way match is in full compliance and the internal person has committed the fraud either alone or in collusion with an external party. To further complicate the matter, the middle company, which is the pass thru company, is either a shell company or a real company. There are over 15 permutations of the pass thru entity scheme. How the scheme operates will also vary by industries.

Shell Company Detection

Shell companies can often be detected by indicators such as

- Missing data associated with the company: no phone number, email address, or physical address (but sometimes a PO Box)
- Vendor invoices missing information that would be normally on the invoice
- Correlating the legal incorporation date to the first invoice date
- Unusual pattern of invoice numbers or dates
- Use analysis of legal background, physical addres, business capacity, background on business owners, and media searches to determine if the company is real.

Ghost Employees

Ghost employees are people on the payroll who don't work for the company in question but do collect a salary or remuneration. This is one of the more common causes of financial loss for a business. The aim of this kind of fraud is for somebody to collect a wage paid to the ghost employee unnoticed. It may also be associated with FCPA bribe payments.

There are three fundamental types of ghost employees and many permutations. The ghost employee is fictitious; real but not complicit and real and complicit in the scheme. To illustrate the concepts, we will discuss the real ghost that is not complicit and the person committing the scheme is the employee's supervisor.

There are two permutations of the real ghost that is not complicit. First, a real employee who left employment some time ago but were kept on the payroll by either payroll office or the budget owner. Second, the real employee was reactivated on payroll by either payroll or the budget owner. Since they are a real person and were a legitimate employee for a time, this kind of fraud is easier to commit.

The key red flag of the scheme is change. Change the address, bank account, where the check is negotiated. The employee was inactive and now is active. The IP address associated with the electronic time record.

Ghost Employee Detection

This kind of fraud is attractive to many fraudsters because on the surface this is a legitimate payroll transaction. There is no need to hide the payroll transaction, only to hide the false information surrounding the ghost employee, and the process of being paid a salary is often not suspicious. Some key red flags to consider with this type of fraud are:

- Timesheets originating from supervisor
- Missing information from employee's files or indeed no personnel file at all
- Little verifiable information as to work performance
- Change of employee master file data: i.e. address, bank acc. or phone number.
- A physical address that is a PO Box
- More than one employee using the same bank account for wages in the same department

Vendor Kickback Scheme

Vendor kickback schemes are commonly known as corporate bribery, with the most recognizable type being overbilling. While there is some divergence in opinions of the form this scheme takes within the fraud community, the existence of overbilling and procurement kickback schemes are generally agreed.

At its most simple vendor kickback schemes are when the owner or employee of one company offers money or other assets to an employee of another company in order to convince them to use a service or product. Most kickback has an element of overbilling to pay for the kickback. The exact fraud scenario will depend on the nature of the goods and services and the industry.

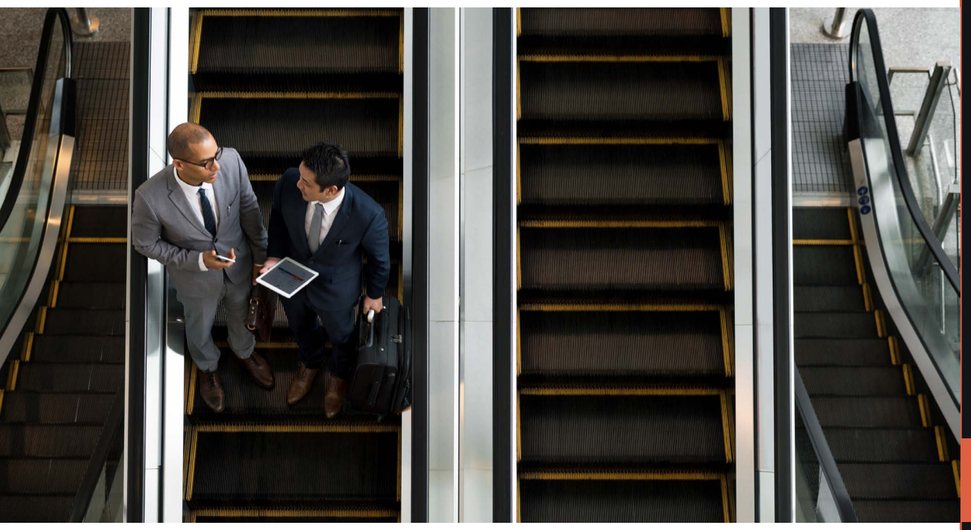
A more sophisticated scheme involves communication to the favored vendor that the actual purchase will differ from the items listed in the request for proposal (RFP). This allows the favored vendor to offer prices on their bid below cost on certain items, because the vendor knows that he will not need to provide the items. Other items where the quantity in the RFP is low, the unit price is high. After the contract is awarded, change orders are issued to accommodate the change in acquisition. The following chart illustrates

Kickbacks occur in many different forms. Many high-profile cases have involved extravagant entertainment or sexual favors. Kickbacks can be interest free loans that never get repaid, use of company assets such as apartments, yachts or sports cars selling of assets below fair market value. The list goes on.

Vendor Kickback Detection

Because of their nature, kickback schemes are generally hard to discern in a company's records. Some common signs of fraud are:

- Prices for goods appearing higher than market value
- Significant changes in the unit prices between vendors
- Employees have an unusual closeness to a particular vendor
- Orders that change in both quantity of item purchased and the mix of products
- Comparison of vendor bids to actual purchases



Sales Representative Pass Through Scheme

During pass through customer schemes, the sales representative at real suppler sets up a shell company and then sells to the shell company at discounted prices. The sale representative then convinces the budget owner at your company to purchase from this shell company versus the real supplier. Your company then places an order with the shell company, the shell company effectively places an order with the real supplier and the real supplier ships directly to the budget owner. The shell company invoices the budget owner at an inflated price. In this scheme both the real supplier and your company suffers losses. The budget owner receives a kickback the sales representative receives fraudulent profits. At first glance, the scheme may seem complicated but once understood the scheme becomes obvious.

Sales Rep Detection

Some common signs of fraud are:

- Shipping address matches another existing customer
- Existing customers that stop purchasing from your company
- Larger customer discounts than other customers for the sales representatives
- Unusually high starting credit limits
- Trend of customer payments being received late

Summary

With each of these schemes, it's becoming increasingly important to adopt a fraud-based approach for detection. While control-based approaches can detect some simple fraud efforts, the more complex fraud schemes and smarter fraudsters will create the illusion that the transaction is legitimate. For example, the address for the ghost employee may be legitimate but only by looking deeper into the real employees for the business will you discover that most of them have no real job titles, and do not come into the office on a regular basis, indicating merit for the suspicion of fraud.

Likewise, an employee might seem legitimate – having a real address, name, and social security number – but only by analyzing patterns in time-sheets coupled with eye witness accounts can you discover they're never where their time-sheets indicate they are. They are a ghost.

Fraud Risk Statement

Fraud risk statements are a good start to a more data driven fraud-based approach to detection and prevention. This section will take a quick look at how the use of Fraud Risk Statements can better improve your prevention techniques.

Fraud Risk Statement

Fraud risk statements can be broken down into five basic components.

1. The person committing the fraud

Identifying the person committing the fraud can start with a very basic description and does not require names. As a rule, we refer to individuals by their job title. It is best to start with a generic description (for example “budget owner”) and narrow this down to a specific role or job title – the more specific this is the better your understanding of the business processes involved. In more complex cases, this element is important for considering direct and indirect access, as well as the impact of internal controls. People play a key part in fraud, so the impact of controls and their access can be pivotal to understanding and preventing fraud.

2. The type of entity

The type of entity depends on the business system. In the expenditure cycle the entity is a vendor, in payroll the entity is an employee, in revenue the entity is a customer. You can also have intangible entities such as inventory sku #.

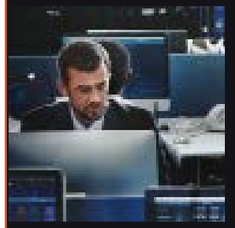
With this description while you similarly start broadly with a description of the business system more complex discussions have over twenty-five difference types of entity. These can be real or fake; much like a vendor or company can be real or fake.

3. Fraud action statement

This describes the act committed by the person involved. For most disbursement fraud schemes primary categories include false billing, pass thru schemes, overbilling, and disguised expenditure schemes. Each primary category can have multiple sub-categories. For example, there are least ten different permutations of the pass thru scheme. Ideally this statement will be adapted based on industry.

4. Impact statement

This statement describes either the monetary or non-monetary impact the fraud will have on the organization.

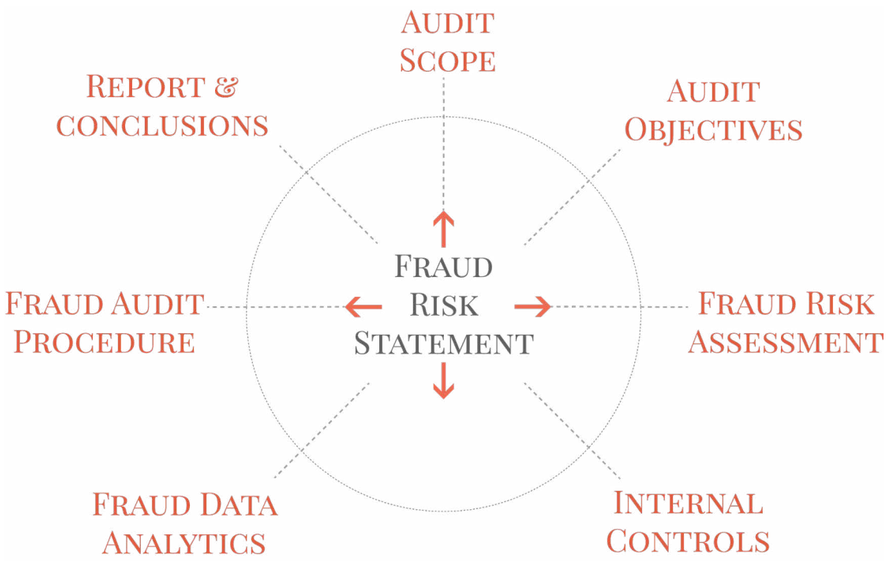


Worked Example

5. Conversion statement

Sometimes we call this a 'believability statement" and this is most useful for conveying the real impact of fraud and how the perpetrator is benefiting from the fraud.

Gathering all of this information makes for a risk statement that goes beyond most risk registers, creating better controls for possible fraud prevention and detection within your company or clients. Fraud risk statements coupled with an understanding of fraud schemes are a good starting point for your fraud plans.



Fraud risk statements are designed to be comprehensive and easy enough that they allow for the immediate creation of a fraud risk register and assist in developing fraud audit programs. The way fraud risk statements feed into your approach to fraud can be seen above.

Worked Example

The number of fraud risk statements for any given organization can be mathematically calculated using the five basic components detailed above. Any time circumstances change you should review the variables to create new statements based on the new situation.

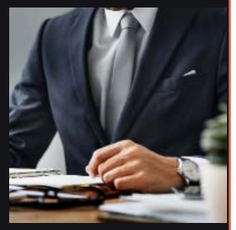
If we take a simple shell company fraud scheme, using the components above we may create a fraud risk statement that follows:

> Budget owner acting alone (person committing fraud) / cause's a shell company (entity) to be set up on the vendor master file (fraud action statement)/ causes the issuance of a purchase order and approves a fake invoice for goods or services not received (fraud impact statement) / causing the diversion of company funds (conversion statement).

Or

> Senior manager acting alone / cause's a shell company to be set up on the vendor master file / causes the issuance of a purchase order and approves a fake invoice for goods or services not received / depositing the funds in an off-book bank account for the purposes of paying a bribe.

While the above example is relatively simple, as stated previously the more specific you get with the person committing fraud and other variables the better your ability to create a fraud plan.



Summary

A fraud risk statement is not how the fraud is concealed or how a perpetrator benefits from a committing a fraud risk statement but rather it is intended to provide fraud auditor with the necessary elements to build their fraud audit program. Recall that in this context the following statements are not fraud risks:

- **Bribery fraud risk.** A bribe is how the person benefits from committing a fraud risk statement, the fraud conversion statement.
- **False document scheme.** A false document is how a perpetrator creates the illusion that the transaction is real, the fraud concealment statement.
- **Fraud concealment.** This correlates to the fraud red flag analysis versus the fraud risk statement. On occasion, describing some aspect of the concealment helps in understanding the fraud risk statement but it is not in itself a fraud risk statement. This is an element of style versus methodology.

A common fraud terminology is essential for creating fraud risk statements and ensures a smoother process when creating fraud audit programs. In the next section we'll take a look at how to further improve your fraud detection using fraud risk identification methodology, all working with common terminology

Fraud Detection & Prevention

In the previous sections we looked at common fraud schemes and starting points for fraud prevention and detection using fraud risk statements. In this section, we'll take a brief look at how fraud risk identification methodology can help improve your fraud detection policies making it easier to identify fraud in areas you might not previously have been able to detect schemes.

Fraud Risk Identification

An effective fraud risk identification process is one that involves a proper understanding of the various factors that must be in place to commit fraud. Fraud risk identification is not any one thing, rather it is an amalgamation of techniques employed to allow your team to better identify and prevent fraud before any fraud has been committed. It is a proactive, rather than reactive, response.

By deploying fraud risk identification into your team's audit plan, you can ensure that when fraud does occur (and it will occur) you are properly equipped to respond and eliminate threats. Within fraud risk identifications there are several key concepts:

- **Fraud Risk Statement Methdology:** An approach to write a fraud risk statement that that uses logic versus life experiences. By using the methodology, the process of fraud risk Identification becomes easier for the audit team. The purpose of the fraud risk statement is to drive the audit process, and to the design the fraud audit test.

- **Fraud matrix:** Your team should use a fraud matrix in their brainstorming session to develop the fraud audit program. The fraud matrix will aid the auditor in the brainstorming by ensuring the completeness of the thought process (person committing, entity, action, and impact). Secondly, how fraud scenario will occur in your business environment and directly link to the concealment, red flags, internal control vulnerabilities and the financial conversion, as well as factors covered in creating a fraud risk statement.

- **Building a fraud audit program:** You will do this based on the mechanics of the fraud risk statement and concealment strategy. A fraud risk statement written using the format described in this eBook, will tell the auditor exactly how to build their fraud audit program

Fraud risk identification should correlate to the fraud risk universe and correlate to the audit scope. There is no need to re-invent the wheel; rather you can use what you have developed previously during the creation of fraud risk statements to expand identification efforts.

It's worth noting that the more detailed your identification is (and the more comprehensive your listing of fraud risk statements are) the more understandable your listings become for management. There is a fine balance when creating a listing of fraud risk statements between creating a comprehensive listing of all statements and ensuring understandability.

When it comes to creating your fraud audit program a key decision is how detailed will you write your fraud risk statements. The advantage of creating a detailed or comprehensive listing of fraud risk statements is to enhance the knowledge of the audit team. Not to worry, it my experience that the same internal control, data mining routine, or fraud audit procedure can address multiple scenarios. Thus, it is essential to truly understand which of these can address which scenarios within your organization.

The necessary level of detail depends on the intended use of the fraud risk statements. When determining which model to use you may consider either entity wide (or macro) level, core business level (micro) level, or fraud penetration (mega-micro) level models. As previously stated, macro level model is intended to identify organization risk, micro level Is for line managers and the micro models is used by fraud auditors to build their audit program.

Creating an Effective Audit Program

Once you have selected a model of fraud risk identification and linked internal controls with fraud risk statements, and created a fraud likelihood score, you can use all your knowledge to create an effective audit program. Your fraud audit approach does not stop here – rather it is the key component of making any audit program. Using the fraud audit approach allows your team to accurately locate and recognize fraud.

Here are some key things to consider when creating your audit program:

1. Fraud Brainstorming for Everyone

IIf you're proactive about fraud data analytics this means continuously monitoring your organization for fraud rather than waiting for the discovery of fraud. Irrespective of your initial approach, reactive or proactive, it's vital that you get staff on-board with a common understanding of fraud risk identification. Often line staff members are your eyes and ears when it comes to detecting fraudulent activity.

Fraud Risk Identification

If the audit team is deploying a fraud-based approach, you're audit team can better understand the internal control vulnerabilities that allows perpetrators to commit fraud. By identifying the red flags and concealment strategies associated with a fraud scenario, the audit team improves the likelihood of detecting the fraud scenario via an audit.

2. Start Fraud Detection Early

Every single level of your organization is vulnerable to fraud. The only truly successful way to detect fraud more efficiently is to make the necessary changes to your approach today, and this means building them into your fraud audit program.

While some organizations approach fraud rather reactively – believing that fraud should reveal itself in due course – it is often the case that fraudsters are smarter than simple controls. Avoiding common red flags and creating entirely new concealment strategies is precisely how fraud schemes can go unnoticed for long periods, resulting in a million-dollar loss versus a small loss.

Hence, it is vital that your team reassess and update their approach to fraud prevention and detection as soon as possible.

If you're concerned about your internal controls or require your team to update their internal controls, perform a review of your fraud risk management program with the help of an external expert. It is often the case that doing this in isolation will result in a brand-new fraud risk program that is still just as capable of missing fraud as its predecessor.

3. When an Investigation Is Necessary, Dig Deep

Any good fraud-based approach is going to detect and prevent fraud schemes more effectively than other approaches in this field.

When an audit is necessary this approach too outshines others. Being able to accurately gather evidence when confronted with complex financial, tax, and accounting data and tell the true story with that information is essential when it comes to any audit.

If you're unsure of exactly where to start with your internal controls or fraud audit plan, there's no need to spend too much time trying to work out which fraud schemes may be lurking in your business system. Pre-prepared fraud risk registers can offer you a comprehensive framework of fraud schemes in your core business systems.

Your audit time can be maximized by understanding how the scheme could occur in your company, focusing on the internal control vulnerabilities that would allow the fraud scheme to occur and building your fraud audit program.

Conclusion

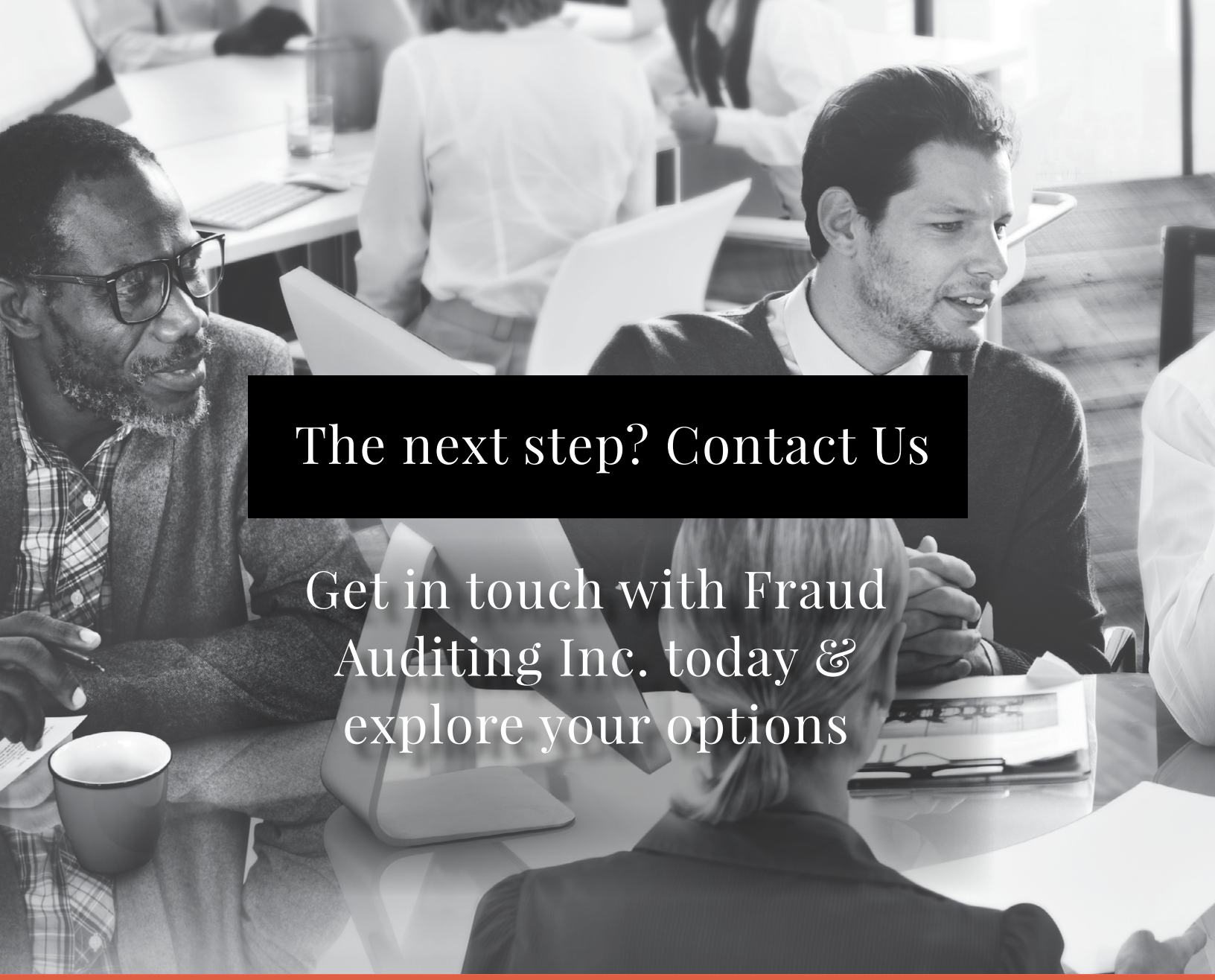
When it comes to fraud, no audit plan is going to fit all. Each fraud risk statement in your audit scope needs its own fraud data analytics plan and fraud audit procedures. An audit plan isn't just a document to create and file away as a matter of process – any auditor involved in future detection and prevention will need this to have the correct information that will allow them to find and reveal which fraud risk statement is occurring.

While no fraud methodology is entirely foolproof, taking a systematic and methodical approach to data by finding hidden patterns and frequency of occurrence is a proven and robust approach to fraud detection.

This eBook has covered a lot of linked ideas, looking into how fraud risk scenario and fraud risk detection procedures are linked processes leading to the creation of more effective fraud audit programs. It is essential to understand the link between all of these, as the stronger that link is in your mind the easier it is to follow your efforts through into any fraud audit program.

A common issue in building fraud audit programs is the tendency to use terminology interchangeably. Hence, in addition to the materials covered in this eBook we recommend your team include within any fraud audit program a document of definitions to allow everyone to understand one another clearly.

Creating a robust fraud audit program that allows you to better locate and recognize fraud is the very essence of improving your fraud prevention and detection procedures. This eBook has provided you with a basic introduction to how you and your team might improve on your current processes to ensure that when fraud does occur your organization is equipped with the tools to find evidence of and deal with that fraud. For more details on how your organization can improve their detection and prevention procedures visit our website at www.leonardvona.com



The next step? Contact Us

Get in touch with Fraud Auditing Inc. today & explore your options