2018 REPORT ON OCCUPATIONAL FRAUD: RESULTS AND HOW COMPANIES CAN PROTECT THEIR ASSETS

Dwight E. Denman
Eastern Oregon University

The Association of Certified Fraud Examiners (ACFE) published their study on occupational fraud and abuse this past year. The study, which is its tenth edition, is the most comprehensive study on occupational fraud and abuse. Its findings give great insight into- among other things- who commits fraud, why they commit fraud, and how companies can protect themselves to deter and detect fraud. This paper will look at the major findings of the study. In addition, the paper will make practical suggestions that companies could implement to deter and detect fraud, with a special focus on internal controls and internal control activities.

Keywords: Fraud, ACFE, Report to the Nations, Internal controls.

INTRODUCTION

A recent study by the Association of Certified Fraud Examiners ("ACFE") *2018 Report to the Nations* (the "report" or the "study" herein), studied 2,690 cases from 125 countries in 23 industry categories. Their findings included the following:

- Of the cases that they studied, there were more than $7 billion in total losses;
- The median loss per case was $130,000;
- 22% of the losses were more than $1 million; and
- The median duration of the fraud scheme was 16 months (Association of Certified Fraud Examiners [ACFE], 2018a).

This paper will discuss the findings in the report, and then introduce the reader to ways that businesses can protect their assets from fraud. Specifically, the paper will discuss internal controls and activities and their importance in preventing fraud. In addition, this paper will discuss the importance of companies adopting a strong anti-fraud policy. Further, the paper will discuss the need for a fraud risk assessment prior to establishing internal controls. Finally, the paper will discuss fraud risk management and an applicable framework associated with it.

WHY DO PERPETRATORS COMMIT FRAUD?

Behavioral Red Flags Found in the 2018 Report

The study found that, of the cases studied, 85% of fraudsters displayed at least one behavioral red flag, and in 50% of the cases there were multiple red flags. The following six red flags were the most common in the 2018 study:

1. Living beyond their means- This behavior was exhibited in 41% of the cases studied.
2. Financial difficulties- This behavior was exhibited in 29% of the cases studied. Of those studied, a larger majority of them were employees, rather than owner/executives- 35% compared to 23%, respectively. Surprisingly, 39% of the perpetrators with this trait were female, while only 24% were male.
3. Unusually close association with vendor/customer- This behavior was exhibited in 20% of the cases studied. Of those studied, a larger majority of them were owner/executives, rather than employee- 24% compared to 16%, respectively. Only 11% of the perpetrators with this trait were female, while 24% were male.
4. Control issues, unwillingness to share duties- This behavior was exhibited in 15% of the cases studied. Of those studied, a larger majority of them were owner/executives-21% compared to 8% employees. No information was given concerning the gender breakdown that exhibited this trait.
5. Divorce/family problems- This behavior was exhibited in 14% of the cases studied. No information was given concerning the perpetrator's position that had this trait. However, 20% of the perpetrators with this trait were female, while only 11% were male.
6. "Wheeler-dealer" attitude- This behavior was exhibited in 13% of the cases studied. Perhaps not surprising was the discovery that a large majority of the perpetrators that showed this trait were owner/executives rather than employees - 22% compared to 8%, respectively. 16% of the perpetrators with this trait were male, while only 6% were female (ACFE, 2018a).

These same six red flags have been the most common in every study dating back to 2008.
In addition to the red flags already mentioned, the perpetrators studied tended to show red flags that related to non-fraud-related conduct and human resources-related conduct.

1. Non-fraud-related conduct- 45% of those studied engaged in non-fraud-related conduct. Of those who showed these other signs, 21% engaged in bullying or intimidation, 14% engaged in excessive absenteeism, and 10% engaged in excessive tardiness.
2. Human resources-related conduct- 39% of the perpetrators experienced negative HR-related issues prior to or during their frauds. Of those who did, 14% experienced poor performance evaluations, 13% had a fear of job loss, and 5% had an actual job loss (ACFE, 2018a).

Note that most perpetrators studied had neither a non-fraud-related misconduct nor a human resource-related behavior reported prior to or during the fraud.

WHO COMMITS FRAUD?

The report looked at several factors involving the cases they reviewed and found several interesting correlations in their findings that relate to the question of who commits fraud. The following are some of those findings.

Position of the Employee

The study found that there was a correlation between the position of the employee in the organization and the amount of the fraud.

1. Employee- 44% of cases the study looked at involved various low-level, non-supervisory employees. The median loss caused by perpetrators in that category was $50,000. The duration of the fraud was 12 months.

2. Manager- Managers made up 34% of the total cases. S150,000 was the median loss, and the duration of the fraud was 18 months.
3. Owner-Executive- Owner/Executives made up 19% of the total cases. The median amount of the losses was $850,000, and the duration of the fraud was 24 months (ACFE, 2018a).

Thus, there was a correlation between the position of the fraudster (level of power), the amount of the fraud, and the length of the fraud. The higher the level of power, the larger the loss and length of time of the fraud. This may be because the higher the fraudster is in the organization, the less likely anyone will question their decisions, and the more trust they will have from those in authority.

Length of Tenure

There was also a correlation between the length of tenure and the amount of loss. The study showed that the longer one was with the organization, the larger the loss. Perpetrators with less than one year of tenure caused a median loss of S40,000, while those with more than ten years' experience at the victim organization caused a median loss of $241,000, more than six times as high. This may be because, the longer the tenure of the employee, the greater knowledge they have of controls and processes in the organization- including gaps or weaknesses in those processes- which may enable them to do a better job of committing and concealing fraud (ACFE, 2018a).

Gender

The study found that the proportion of male fraudsters went up with their level of authority. At the employee level, only 58% of the fraudsters were male, but that number increased to 73% for managers and 86% for owners/executives. The study also found that males tended to cause significantly larger losses than females in owner/executive roles. Male owners/executives caused a median loss of $1 million, as opposed to a median loss of $295,000 caused by female owners/executives (ACFE, 2018a).

Age

The study showed that losses tended to rise with the age of the perpetrator. The largest median loss in the study were caused by those in the oldest age ranges (56 and older), while those perpetrators 30 or younger caused a much smaller amount of damage. The median loss for those between the ages of 56-60 was $480,000, whereas the median loss for those 26-30 was $40,000 (ACFE, 2018a). This factor may be because older perpetrators tend to hold a higher position in the organization, as well as a longer tenure.

Level of Education

The study showed there is also a correlation between the fraudster's education level and the size of the fraud. Those with a postgraduate degree caused a median loss of $230,000, and those with a bachelors' degree caused a median loss of $160,000. Both these figures were much higher than the median loss of schemes by fraudsters with a high school degree or less ($75,000) (ACFE, 2018a).

The study suggests that reasons for these differences may indicate that highly educated fraudsters have superior technical abilities or knowledge that make them more effective at committing fraud, but it is also probably influenced by the fraudster's position of authority. More highly educated individuals tend to occupy higher positions within an organization. For example, the study showed that approximately 68% of those with a university or postgraduate degree were either managers or owners/executives (ACFE, 2018a).

Criminal Background

The study showed that a vast majority of the perpetrators had no prior history of criminal fraud convictions. Only 4% of the perpetrators in the 2018 study had previously been convicted of a fraud-related offense, which is consistent with findings in every study dating back to 1996. This suggests that most occupational fraudsters are first-time offenders. However, between 58% and 69% of occupational fraud cases in their past studies were never referred to law enforcement, which indicates that the actual number of repeat offenders is probably higher than what can be identified through conviction records (ACFE, 2018a).

Employment History

The study showed that 85% of the occupational fraud perpetrators had never been punished or terminated for fraud-related conduct prior to the crimes in the study. This tends to indicate that most occupational fraudsters are first-time offenders, but as with criminal conviction data discussed earlier, this data might understate the real number of repeat offenders. 28% of perpetrators in the study either received no punishment from their employers, were permitted to resign, or entered into private settlement agreements (which are typically confidential). Therefore, the true number of repeat offenders may be higher than what is indicated by employment background checks. In addition, 85% of the perpetrators had no prior disciplinary actions with the victim organization in the study (ACFE, 2018a).

Perpetrator's Department

The study showed that 77% of perpetrators in the study came from just 8 departments: accounting, operations, sales, executive/upper management, customer service, administrative support, finance, and purchasing. Accounting and Operations were each responsible for 14% of the frauds in the study, but the median loss caused by those in the accounting department ($212,000) was significantly larger than the median loss from operations ($88,000). Frauds committed by those in executive or upper-management roles were slightly less common, but much costlier. They accounted for 11% of the cases but caused a median loss of $729,000 (ACFE, 2018a).

The perpetrator's department showed a correlation between the department and the fraud scheme that was committed. For example, in the accounting department, 29% of the frauds committed were billing schemes, and 30% were check and payment tampering. For executive/upper management, 62% were corruption-related, whereas 35% were billing-related (ACFE, 2018a).

Collusion by Multiple Perpetrators

Approximately half of the cases studied involved multiple perpetrators who collude with one another to commit fraud. Fraud losses rose significantly when more than one fraudster was involved in a scheme. The median loss with one fraudster involved was $74,000; with two perpetrators, it rose to $150,000. With three or more perpetrators, the median loss rose to $339,000. One likely explanation for this finding is that many anti-fraud controls work on the principles of separation of duties and independent checks. When multiple perpetrators conspire in a fraud scheme, they can circumvent the system of independent verification that might otherwise detect fraud (ACFE, 2018a).

HOW IS OCCUPATIONAL FRAUD COMMITTED?

The report showed that there were three primary categories of occupational fraud- asset misappropriation, corruption, and financial statement fraud. Of the three, asset misappropriation was the most common at 89% of the cases and a median loss of $114,000. Corruption was the next most common, accounting for 38% of the frauds and a median loss of $250,000. By far the least common- but this highest median loss- was financial statement fraud. It accounted for only 10% of the frauds, but the median loss was $800,000. Many of the frauds studied involved more than one fraud scheme. The authors of the study suggest that fraudsters typically seize whatever opportunity arises when committing their schemes (ACFE, 2018a).

Asset Misappropriation Sub-schemes

Within the asset misappropriation category, the study showed several distinct subcategories of schemes. They identified the nine main sub-schemes they found on a heat map and listed the median loss, the frequency of occurrence, and its relative riskiness. Of the nine, three categories stood out.

1. Check and payment tampering- This subcategory had a median loss of $150,000 and was 12% of all the subcategories. It was listed as being moderately risky.
2. Billing schemes- This subcategory had a median loss of was $100,000 and was 20% of all the subcategories. It was listed as being risky.
3. Theft of Noncash Assets- This subcategory had a median loss of was $98,000 and was 21% of all the subcategories. It was listed as the riskiest of all the subcategories (ACFE, 2018a).

Corruption

Of the cases studied, 70% of the perpetrators were in a position of authority- 32% of the perpetrators were owners/executive, while 38% were managers. 82% of the perpetrators were male, and only 18% of them were female. The top red flags in these cases were living beyond their means (43%), unusually close association with a vendor/ customer (34%), financial difficulties (23%), and wheeler-dealer attitude (21%). The highest proportion of corruption was in three industries: energy (53%), manufacturing (51%), and government and public administration (50%) (ACFE, 2018a).

Financial Statement Fraud

Financial statement fraud accounted for the least common fraud perpetrated fraud at 10% of the cases, but the costliest at a median loss of $800,000. A total of 27% of the owner/executive frauds were financial statement frauds (ACFE, 2018a). It makes sense that owner/executives would perpetrate the bulk of financial statement frauds, since these individuals:

- possess the power and knowledge to override controls- if any- to perpetrate the fraud
- possess the power to order underlings to assist then in perpetrating the fraud
- possess the power and knowledge to hide the fraud from auditors and perpetuate it longer.

These statistics also correlate with the fact that owners/executives accounted for a small percentage of fraud cases (19%), caused a median loss of $850,000, and the duration of the fraud was 24 months (ACFE, 2018a).

HOW OCCUPATIONAL FRAUD WAS DETECTED AT VICTIM ORGANIZATIONS

Understanding the methods by which occupational frauds are detected is critical for both investigating schemes and implementing effective prevention strategies. In the study, participants were asked to tell the authors how the frauds they investigated were initially detected. The results indicated that the leading detection methods were tips, internal audits, and management reviews. These three methods have been the three most common means of detecting occupational fraud in every edition of the report since 2010. Collectively, these three detection methods were cited in 68% of the cases in the study. Of these three methods, tips were the most common at 40% of the cases, internal audits were 15%, and management reviews were 13% (ACFE, 2018a).

The study found that the median duration and median loss were relatively low in frauds that were detected by active methods. For instance, frauds detected actively by IT controls tended to last five months and cause a median loss of $39,000. In comparison, frauds detected by external audits (categorized as potentially active or passive detection method) lasted between 15 and 20 months; schemes detected passively through notification from law enforcement last two years and caused a median loss of almost $1 million (ACFE, 2018a).

Tip Sources

Since tips are the most common detection method, it is important to understand where those tips come from. 53% of the tips were provided by employees of the victim organizations, 32% of the tips came from people outside the organization (customers, vendors, and competitors), and 14% came from an anonymous source (ACFE, 2018a).

The authors noted that, while active cultivation of tips and complaints (such as the promotion of fraud hotlines) are geared toward employees, the data suggest that organizations should consider promoting reporting mechanisms to outside parties, especially customers and vendors. The authors also noted that since 14% of tips came from anonymous sources, this demonstrated that a significant portion of those who reported fraud did not want their identities known. The reason, according to the authors, is that they fear being identified and retaliated against. Thus, the authors stress that it is important that these tipsters be able to make reports anonymously where the practice is legally permissible (ACFE, 2018a).

Tips and Fraud Hotlines

The study found that 63% of the victim organizations utilized tip hotlines. Of those who had hotlines, 46% of cases were detected by tips, compared with only 30% of cases detected by tips at organizations that did not utilize hotlines. In addition, losses at organizations who utilized hotlines were smaller- $100,000 compared to $200,000 for those organizations that did not utilize hotlines. Moreover, organization without hotlines were twice as likely to detect fraud by accident or external audit (ACFE, 2018a).

The study also looked at the percentage of the three major categories of occupational fraud- asset misappropriation, corruption and financial statement fraud- that were detected by a tip. What they found is that corruption was particularly likely to be detected by tip- at 50%. In addition, they found that 38% of asset misappropriation was detected by tip, and 38% of financial statement fraud was detected by tip (ACFE, 2018a).

The study also found that not all tips came through hotlines. It found that, when a reporting mechanism was not utilized by a company, 32% of the tips came from direct supervisors, 15% came from an executive, 13% came from a fraud investigation team, 12% came from a coworker, and 10% came from an internal audit (ACFE, 2018a).

DURATION OF FRAUD SCHEMES

The median duration for all the fraud cases in the study was 16 months. However, the authors noted, it stands to reason that the longer a fraud scheme goes undetected, the larger the scheme will grow. The study showed that frauds that lasted over 60 months were more than 20 times as costly as those that were caught in the first six months ($715,000 compared to $30,000, respectively). The authors stated that their data also indicated that fraudster tended to start small and increase their frauds rapidly over the first three years. Thus, the authors concluded, it is important for organizations to implement proactive fraud detection mechanisms to catch frauds quickly and minimize their damage (ACFE, 2018a).

Payroll schemes were the longest-lasting schemes, with a median duration of 30 months. Check and payment tampering, financial statement fraud, expense reimbursements, billing, and cash larceny all lasted a median average of 24 months. Corruption lasted a median duration of 22 months (ACFE, 2018a).

Median Loss and Duration by Detection Method

The study also analyzed the median loss and duration of fraud schemes based on how they were uncovered. The authors of the study concluded that there was a correlation between the way in which occupational fraud schemes are detected and the severity of the fraud. They also concluded that the data points to steps that organizations can take to detect fraud proactively and, in doing so, mitigate losses.

The authors categorized detection methods into three categories: Active method, potentially active or passive detection method, and passive detection method. Active detection methods involve a deliberate search for misconduct from someone within the organization or an internal control designed to detect fraud. Passive detection methods refer to cases in which the organization discovers the fraud by accident, confession, or unsolicited notification by another party. The study classified tips and external audits as potentially active or passive detection methods because those mechanisms might or might not involve proactive efforts to specifically identify fraud, depending on the circumstances (ACFE, 2018a).

Concealment of Fraud

An act of fraud typically involves not only the commission of the fraud, but also efforts to conceal the misdeeds. Understanding the methods fraudsters use to cover their crimes can help organizations better design prevention mechanisms and detect the warning signs of fraud. The study found that, in only 3% of cases studied did the fraudster not attempt to conceal their fraud. Of the cases that were unconcealed, all the frauds were committed by owners/executives.

The eight top concealment methods used by fraudsters were the following:

- Created fraudulent physical documents- 55%
- Altered physical documents- 48%
- Created fraudulent transactions in the accounting system- 42%
- Altered transactions in the accounting system- 34%
- Altered electronic documents or files- 31%
- Destroyed physical documents- 30%
- Created fraudulent electronic documents or files- 29%
- Created fraudulent journal entries- 27%

In 63% of the cases, both electronic and physical evidence were concealed, while 21% involved only electronic evidence and 12% involved only physical evidence (ACFE, 2018a).

MAKEUP OF VICTIM ORGANIZATIONS

More than 70% of the frauds in the study occurred at for-profit organizations, with 42% of the victim organizations being private organizations and 29% being public companies. The private companies in the study suffered the greatest median loss, at $164,000. Not-for-profit organizations were the victim in only 9% of frauds and had the smallest median loss of $75,000; however, for many not-for-profit entities, financial resources are extremely limited and a loss of $75,000 can be particularly devastating (ACFE, 2018a).

Size of Organization

The size of the organization can directly affect both the opportunity for fraud and the ability to enact certain anti-fraud mechanisms. Larger entities typically have more resources to invest in the anti-fraud programs, as well as a greater ability to separate duties among staff members to help prevent fraud. However, a large staff size can also mean more potentially dishonest employees who might attempt schemes and more complex processes and transactions, which can increase the risk of fraud (ACFE, 2018a).

The study analyzed cases based upon the size of the victim organizations. What they found is that small organizations (those with less than 100 employees) suffered both the greatest percentage of cases in their study (28%) and the greatest median loss ($200,000). In comparison, organizations with 100 to 999 employees made up 22% of the organizations in the study and suffered a median loss of $100,000; organizations with 1000 to 9999 employees made up 26% of the organizations in the study and suffered a median loss of $100,000; and organizations with at least 10,000 employees made up 24% of the organizations in the study and suffered a median loss of $132,000 (ACFE, 2018a).

The study also showed that 42% of frauds in small organizations were due to the lack of internal controls. The authors of the study suggest that these organizations have fewer resources to both prevent and recover from a fraud, and they often require an increased level of trust in employees due to a lower ability to implement robust anti-fraud controls. The study also noted that small organizations detected the fraud via tip in 29% of the cases, while organizations of 100 or more uncovered fraud by tip in 44% of the cases. The study also found that owners/executives in small organizations perpetrated 29% of the frauds, whereas only 16% of the frauds in organizations with 100 or more employees committed the fraud (ACFE, 2018a).

Industry of Victim Organizations

The study further examined the cases based on the industry of the victim organization. They found that the greatest number of cases in their study came from banking and financial services, manufacturing, and government and administration sectors. The authors note that these industries are the most likely to employ certified fraud examiners, and thus may uncover fraud more often, rather than the industries that are most susceptible to fraud. The top three industries with the highest median loss were communications and publishing (median loss of $525,000 but only 27 cases), energy (median loss of $300,000 and 94 cases), and manufacturing ($240,000 median loss and 212 cases) (ACFE, 2018a).

The schemes used by the fraudsters varied among industries. In a vast majority of the industries, corruption cases posed the greatest threat. For example, in the banking and financial services industry the highest percentage of fraud was due to corruption, at 36%. The same is true for the manufacturing and energy industries; in manufacturing, corruption cases were 51% and energy had 53%. The second highest percentage of fraud schemes were either billing schemes or noncash theft of assets, depending on the industry. In manufacturing, billing made up 27% of the frauds reported, whereas in the same industry noncash theft made up 28% of the frauds. In the retail industry, however, noncash theft was 34% of the frauds reported, whereas billing schemes only made up 20% of the cases (ACFE, 2018a).

ANTI-FRAUD CONTROLS UTILIZED BY VICTIM ORGANIZATIONS

The study then analyzed the anti-fraud controls of the victim organizations to see which ones were most effective. The authors of the study suggested that organizations can benefit from knowing which anti-fraud controls are commonly used by their peers, as well as which tend to be most effective. The authors supplied the respondent organizations with a list of 18 anti-fraud controls and asked which, if any, were present at the victim organization at the time the fraud occurred. What they found is that 80% of the organizations had a code of conduct and underwent external financial statement audits, 73% had internal audit departments, and 72% had company management certify the financial statements. However, only 19% of organizations had policies requiring job rotations/mandatory vacations, and only 12% provided rewards for whistleblowers (ACFE, 2018a).

Effectiveness of Anti-fraud Controls

The authors acknowledged that demonstrating the return on investment in anti-fraud initiatives was a difficult task, as it is nearly impossible to measure the amount of fraud prevented by a specific control. To provide some insight into the relative effectiveness of various anti-fraud controls, the authors compared the losses experienced by the victim organizations that had specific controls in place against the losses experienced by those that had not implemented Those specific controls. What they found is that the presence of every control they analyzed was correlated with lower fraud losses. For example, the use of proactive data monitoring and analysis and surprise audits were associated with a more than a 50% reduction in fraud losses. However, the study found that, of the companies they surveyed, only 37% of them used proactive data monitoring and analysis and 37% used surprise audits (ACFE, 2018a).

The study also analyzed the duration of fraud schemes based on the presence or absence of each anti-fraud control. What they discovered was that data monitoring and surprise audits were correlated with the most significant reductions in fraud duration. The authors concluded that as these controls were also associated with some of the largest loss reductions, which indicates that they are among the most useful tools in the fight against fraud (ACFE, 2018a).

Internal Control Weaknesses that Contributed to Fraud

Understanding the factors that can lead to fraud is also a key in preventing future occurrences. The study asked survey respondents what they perceived to be the primary internal control weakness that contributed to the fraud they reported. The authors found that, in 30% of the cases, a simple lack of controls was the main factor while 19% of the cases occurred because the perpetrator was able to override the controls that had been put in place (ACFE, 2018a).

The authors further analyzed these control weaknesses based on the category of fraud involved in the scheme. What they found was that a poor tone at the top was much more likely to be the primary factor in financial statement fraud and corruption cases than in asset misappropriation cases. However, they noted that a lack of internal controls is more common in asset misappropriation and financial statement frauds while corruption schemes are more likely than other schemes to involve an override of existing controls. The study also found that a lack of management review was the main reason for asset misappropriation schemes than other forms of fraud (ACFE, 2018a).

HOW VICTIM ORGANIZATIONS REACTED TO DISCOVERY OF THE FRAUD

The authors of the study asked the victim organizations about what happened after the organization had determined that a fraud had occurred. The most common disciplinary action taken against the perpetrator was termination in 65% of the organizations. Surprisingly, though, over one-third of the organizations did not terminate the perpetrator as a result of committing fraud. In 12% of the cases, a settlement agreement was reached; in 10% of the cases, the perpetrator was permitted or required to resign; in 8% off the cases, the perpetrator was placed on probation or suspension; and in 6% of the cases, there was no punishment issued at all (ACFE, 2018a).

Frequency of Criminal Prosecution and Civil Suits

After a fraud has been discovered and investigated, the cases might proceed to criminal prosecution, civil litigation, both, or neither. There are many factors that can affect this result, such as the amount of financial loss, the strength of the evidence, and prosecutorial discretion. The authors of the report further looked at the percent of cases that were referred to law enforcement or resulted in a civil suit being filed for each of their studies dating back to 2008. What they discovered is that the rate of criminal referrals has gradually decreased over that time, from 69% in 2008 to 58% in 2018. In contrast, the rate at which civil suits are filed has remained consistent, ranging from 22% to 24% within the same timeframe (ACFE, 2018a).

Results of Criminal or Civil Litigation

The authors also looked at the results of any criminal prosecution or civil litigation pursued. On the criminal side, most cases that were referred to law enforcement ended in a plea agreement or a conviction at trial (73% combined). If a case was referred to law enforcement and did not end in a conviction, it was likely because law enforcement declined to prosecute (18%). The results indicate that once law enforcement decides that it will proceed with prosecution, it has an overwhelming chance of securing a conviction; only 1% of defendants avoided a conviction (ACFE, 2018a).

Reasons for not Referring Cases to Law Enforcement

There are many reasons why a victim organization might not want to refer a fraud for criminal prosecution. In the study, the top cause cited was fear of bad publicity (38%), followed by internal discipline being sufficient (33%), costliness (24%), and private settlement agreement (21%) (ACFE, 2018a).

Recovery of Fraud Losses

After a fraud has been detected, the victim organization might try to recover its losses from the fraudster or other sources. The data shows that victims are rarely made whole. In 53% of the cases, the victims recovered nothing; in 32% of the cases, the victims received a partial recovery; and in 15% of the cases, the victims recovered all their losses. When breaking it down into categories according to the size of the loss, the results showed that the more that the victim lost, the less likely they were to make a full recovery. For example, when the victim lost less than $10,000, they were able to make a full recovery in 30%of the cases, whereas in cases where the loss was $100,001-$1,000,000, only 13% of the victims made a full recovery. It gets even worse when the losses exceed $1,000,000, where only 8% of the victims were able to make a full recovery (ACFE, 2018a).

PREVENTION AND DETECTION OF OCCUPATIONAL FRAUD

Internal Controls

The study found that internal control weaknesses were responsible for nearly half of the frauds in their study. In addition, in 30% of the cases lack of controls were cited (ACFE, 2018a).

Research suggests that companies that have material weaknesses in internal controls have significantly lower gross margins and are smaller when compared to a set of control firms matched by industry (Srinivasan, R. and Cornelsen, E., 2017).

Another study has found that material weaknesses in internal control design and control environment have the greatest impact on a company's return on assets (Lai, Y., Li, H., Lin, H., and Wu, F., 2017). Another recent study concluded that effective internal control not only helps external market participants make more informed decisions, as documented in prior research, but also enhances the firms' internal operations (Cheng, Q., Goh, B.W., and Kim, J.B., 2018). Therefore, it is incumbent on companies to establish and monitor proper internal controls.

It is management's job to ensure that the proper internal controls are in place to safeguard assets from fraud. These controls must continually be monitored to ensure that the proper internal controls are adopted, implemented and working as intended. to make sure that they prevent, detect, or correct fraud, depending on the intent of management in adopting a specific control.

Internal controls may be either a general control or an application control. A general control relates to a control that addresses entity-wide issues dealing with internal controls, such as user access to the entity's information system. An application relates to a specific subsystem or application to ensure the validity, completeness, and accuracy of certain transactions. For example, when entering a sales transaction, the use of an input control ensures the customer account number is entered accurately.

For publicly-held companies, the Sarbanes-Oxley Act of 2002 requires that these companies use a recognized internal control framework in determining the proper controls to adopt, such as the framework developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. The framework can also be useful to non-public companies in establishing a strong internal control program. According to the framework, "internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance." (COSO, 2013, p. 3).

To meet these objectives the framework identifies five components of internal control. They are:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring (COSO, 2013).

In addition, there are seventeen principles within those 5 components. The objectives and principles listed in the framework are meant to guide those stakeholders in the entity in ensuring that the proper internal controls are adopted and implemented so that the entity can achieve their operating, reporting, and compliance objectives.

Control Activities

One of the central components of the framework to ensure that the proper internal controls are adopted and implemented are control activities. Control activities are the policies and procedures that enforce management's directives to mitigate risk. These actions are performed at all levels of the organization, at all stages of business processes, and through both manual and automated procedures. They can be designed to prevent the occurrence of risks, detect the occurrence of risks, or both.

Management must make sure that:

- Controls are selected and developed to help reduce risks to an acceptable level;
- Appropriate general controls are selected and developed over technology; and
- Control activities are implemented and followed as specified in company policies and procedures (Romney M., and Steinbart, B., 2015, p. 204).

However, before internal controls and activities can be initiated in an organization, the organization must be committed to adopting an anti-fraud policy and complete a fraud risk assessment. Once these things have been done, then the organization can adopt those internal controls and control activities that are deemed necessary for the organization to meet its objectives.

FRAUD PREVENTION AND RISK MANAGEMENT

Initiating an Anti-Fraud Policy

The first thing that must happen before any anti-fraud policy program can be implemented is that the directors and management must have be dedicated to preventing and detecting fraud. One would think that such dedication would be without much thought- however, there may be reasons why those in charge may not be sold on such a program.

Management may not think that internal fraud is a real problem. However, in the ACFE's 2018 Report to the Nations, a survey among over 2,000 Certified Fraud Examiners indicated that the respondents thought that organizations lose an average of five percent of revenues to fraud each year. This is a huge number- one that may be the difference between a company continuing or folding in these days of ever-decreasing margins. Fraud affects net sales dollar for dollar. For example, if a company nets 20 percent on sales, it must sell five items at regular prices to recover losses (cost plus lost profit) from the theft of one item. This removes several trillions of dollars in profits from the world economy each year.

Management may not think that their employees are capable of fraud, and even if they have had a few past incidents of fraud, it is not widespread throughout the organization. Or perhaps they think that most of their employees are "honest." However, the ACFE has estimated that as much of one-third of all employees in an organization would commit fraud, if they had the opportunity (ACFE, 2018a).

Anti-Fraud Policy

Once the idea of an anti-fraud program has been sold, the next step is usually for the directors and management, along with other key players in the organization, to set up an anti-fraud policy for the organization. The policy may be a stand-alone policy, or it can be included in a broader Code of Ethics. While the details of the policy may vary from company to company, there are some basic topics that should be covered in each one.

1. Defining Fraud- Each anti-fraud policy should post the definition of fraud so that each employee knows what it is. Since definitions are often too general for the layman employee to grasp, it is also a good idea to include examples of some of the more common acts that constitute fraud.

2. Source and Scope of Policy- The policy should indicate that the policy is coming from the board of directors and top management to show that they are setting the tone for not tolerating fraud in the organization. Lower level employees must know that they have established the policy and that the policy applies to all employees at all levels, as well as the directors (ACFE, 2018b). A morale-crusher for a company is when there is one standard for the lower-level employees, and another for the executives and directors. The policy should also indicate that, while management may have the ultimate responsibility for preventing, detecting, and reporting fraud, it is the responsibility of everyone in the organization to help prevent, detect, and report fraud (ACFE, 2018b).
3. Reporting Fraud- The way fraud is reported may vary by company, usually due to individual characteristics of the company, such as its size. However, the company should explicitly state in the policy the procedures for reporting fraud. Companies may want to have a hotline for reporting fraud, which may be managed either internally or externally. Companies may want an employee or department to be referred to in the policy for reporting fraud, such as the internal audit or security department. The policy should also indicate that the reporting party will remain anonymous and not be disclosed to any outside parties (ACFE, 2018b).
4. Consequences- The policy should indicate the range of consequences that may occur to anyone who is caught committing fraud. Consequences should include a wide array of actions, including disciplinary action, termination, civil suits to recover damages, and reporting the fraudster's actions for criminal prosecution. In other words, management should forcefully state that they have a zero-tolerance policy for fraudulent activity (ACFE, 2018b).
5. Investigating Authority- The policy should indicate who is responsible for investigating all allegations of fraud. This may be an individual, a group such as a committee that management has given authority to, or a department such as internal audit or the security department (ACFE, 2018b).
6. Communicating the Policy- The policy could be communicated several ways, either in groups of separately. However, multiple ways of communicating the policy is probably a better way to reinforce the policy and make employees realize that management is serious about preventing and detecting fraud.
    - Posters- These could be placed prominently in each breakroom or bulletin board, as well as on the company's website.
    - Training Seminars- Implementing the policy could be followed by a seminar with employees to go over it and discuss it, as well as go more in-depth on what acts constitute fraud.
    - Individual Meetings- Each employee could meet with either the committee or their superior and be presented with the policy. While this is more time-consuming, it may be more effective (ACFE, 2018b).

FRAUD RISK ASSESSMENT

Once management has determined the need to establish an anti-fraud policy, the next step is for management to assess the organization's risk of fraud. There are various risk assessment frameworks that an organization could utilize. For convenience, this paper will introduce the framework that the ACFE has created.

Why Conduct a Fraud Risk Assessment?

The organization cannot prevent and detect fraud unless they first know what the company's vulnerabilities are. Every company has weaknesses- both inherent and residual- that may be subject to fraud. The inherent risk of a company is risk that exists in a company without consideration for internal controls. Among some of the factors in inherent risk are the type of industry the company is in, management style, and the inherent fraud risk in certain accounts- such as cash- which is highly sought out by fraudsters. The residual risk is the fraud risk that exists after the effect of the company's internal controls (ACFE, 2018b).

The Fraud Assessment Team

The company must establish a team of individuals to prepare, disseminate, evaluate the results of the risk assessment framework, and (eventually) implement the fraud risk management strategy. The team should consist of all key players in the organization who have considerable knowledge in determining where significant fraud risks lie, as well as those who have a stake in advising on policies, procedures, legal ramifications, and implementation and enforcement issues. Such players may vary by company, but the following players should be considered:

- Independent directors
- Key management
- Human resources
- Internal audit
- Security
- Information technology
- Legal (ACFE, 2018b).

Once the team is determined, then the team must come up with a means of determining where the inherent and residual risks in the company are greatest. Many companies use one of the various fraud risk assessment frameworks that are available.

Fraud Risk Assessment Framework

Companies can ensure that they are achieving the best assessment of risk by using one of the established risk frameworks. The ACFE has established one, creatively entitled the Fraud Risk Assessment Tool (FRAT). The FRAT consists of 15 modules, each containing a series of questions designed to help organizations zoom in on areas of risk. The ACFE's Fraud Risk Assessment tool is an invaluable resource for fraud examiners and team members to use in identifying and addressing their clients' or employers' vulnerabilities to internal fraud. Fraud professionals and team members can use this tool to assist organizations in identifying fraud risks and developing a fraud risk response. Each Module contains instructions, a questionnaire, and a key to interpreting the responses on the questionnaire. Each module can be dispersed to each functional area covering the model so that the personnel in that group can respond to the survey questions (ACFE, 2018b).

Once the feedback has been completed on each module, the assessment team can begin the work of determining which of these areas pose the greatest risks to the company. They must:

- Identify potential inherent fraud risks and schemes;
- Assess the likelihood of occurrence of the identified inherent risks;
- Assess the significance of each inherent fraud risk to the organization;
- Evaluate which people and department are most likely to commit fraud;
- Identify and map existing preventive and detective controls to the relevant fraud risks;
- Evaluate whether the identified controls are operating effectively and efficiently; and
- Identify, evaluate and respond to residual fraud risks that need to be mitigated (ACFE, 2018b).

The ACFE has a handy tool that companies can use- the Heat Map- to plot the significance and likelihood of each significant threat that is identified. There are 4 quadrants and 2 factors (one of the factors is on the x-axis, and the other is on the y-axis): 1.) Significance of the threat, and 2.) Likelihood of threat occurring. Each identified risk is placed on the quadrant, based upon whether the significance of the threat is high or low, and whether the likelihood of the occurrence is high or low. The team should mainly concentrate of those risks that are both highly likely to be significant and highly likely to occur. Once these risks have been addressed, then the team may want to address those risks that are both likely and significant (ACFE, 2018b).

Regardless of the framework used to conduct the fraud risk assessment, management must address the identified risks to ensure that the organization is within the established tolerance level for fraud risk (ACFE, 2018b).

FRAUD RISK MANAGEMENT

After the team has received feedback and have identified those risks that are both likely to be significant and likely to occur, then the team must determine how they are going to manage those risks. Just as with the fraud risk assessment phase, many companies use an established framework to help assist them in managing risk. This framework that the company uses assists the company in determining the policies and procedures that the company should incorporate as part of their internal control system over those parts of the company that were deemed to have insufficient controls while also showing a significant risk.

Fraud Risk Management Frameworks

The most widely used Risk Management framework is the COSO Enterprise Risk Management-Integrated Framework (COSO ERM 2004), published in 2004. COSO ERM 2004 defines enterprise risk management as "a process … designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO, 2004, p. 2).

Risk management involves the identification, prioritization, treatment, and monitoring of risks that threaten an organization's ability to provide value to its stakeholders, whether increasing profitability and shareholder value for a for-profit entity or achieving program-specific goals for a nonprofit or governmental agency. More specifically, risk management balances risk appetite- how much risk management is willing to accept- with the ability to meet the organization's strategic, operational, reporting, and compliance (COSO, 2004).

COSO ERM 2004 builds upon the five components first identified in COSO's Internal Control-Integrated Framework and includes an additional three components. The eight components of the COSO ERM 2004, and explanations of each, are:

- Internal environment- Encompasses the tone of an organization and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- Objective setting- Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives, and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- Event identification- Internal and external events affecting the achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
- Risk assessment- Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and residual basis.
- Risk response- Management selects risk responses- avoiding, accepting, reducing, or sharing risk- developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- Control activities- Policies and procedures are established and implemented to help ensure that the risk responses are effectively carried out.
- Information and communication- Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities.

Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

- Monitoring- The entity of enterprise risk management is monitored, and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both (COSO, 2004, pp. 3-4).

Implementing a Fraud Risk Management Program

1. Preventative and Detective Internal Controls and Activities/Procedures

   After assessing an entity's risks of fraud and determining how the entity decides to manage fraud risk, the entity incorporates certain internal controls to assist them in preventing and detecting fraud. The internal controls that a company chooses to incorporate depends on their assessment of the entity's risks; therefore, the internal controls that an entity chooses to utilize in managing fraud risk is unique to the entity. Control activities are policies, procedures and rules that provide reasonable assurance that control objectives are met, and risk responses are carried out. Management must make sure that 1.) controls are selected and developed to help reduce risks to an acceptable level, 2.) appropriate general controls are selected and developed over technology, and 3.) control activities are implemented and followed as specified in companies and procedures.

   Control activities/procedures come from the following categories:

   - Proper authorization of transactions and activities- Specific or general authorization for a party given authorization to allow a transaction to occur.
   - Segregation of duties- Functions of authorization, recording, and custody are separated in important functional areas, such as accounting.
   - Project development and acquisition controls- Methodology to govern the development, acquisition, implementation, and maintenance of information systems.
   - Change management controls- Controls to ensure that changes in existing systems to reflect new business practices do not introduce errors or facilitate fraud.
   - Design and use of documents and records- Proper design and use of electronic and paper documents and records help ensure the accurate and complete recording of all relevant transaction data.
   - Safeguarding assets, records and data- Establishing computer controls to safeguard assets, maintaining accurate records of all assets, restricting access to assets, and protection of records and documents.
   - Independent checks on performance- Independent checks on transactions, by someone other than the one who originally performed the transaction, to help ensure that they were processed accurately (Romney M., and Steinbart, B., 2015).
2. Monitoring- Once internal controls are adopted and implemented, they must be continuously monitored, evaluated and modified to make sure they are working as desired. Methods for monitoring performance of internal controls include the following:

   Perform internal control evaluations

   - Implement effective supervision
   - Use responsibility accounting systems
   - Monitor system activities
   - Conduct periodic audits
   - Install fraud detection software
   - Implement a fraud hotline
   - Hire a chief compliance officer (Romney M., and Steinbart, B., 2015).
3. Other Considerations- In support of the implementation and monitoring of internal controls, there are other things that companies can do to support internal controls:

- Human Resources Practices- The organization should make sure that they have the proper policies and procedures in place for hiring, discipline and firing of employees, including criminal background checks and verification of degrees, certifications, and other credentials.
- Communication of anti-fraud policy and follow-up with proper discipline for any discovered fraud- Management should communicate to employees that fraud will not be tolerated at any level of the company. To back that up, management must take the appropriate action against any fraud that is discovered to show their commitment to fighting fraud, including criminal prosecution (Romney M., and Steinbart, B., 2015).

CONCLUSION

The results from the 2018 *Report to the Nations* indicate that fraud is as prevalent as it ever was-possibly even more so. For that reason, it is incumbent on directors and senior management to find ways to prevent and detect fraud. It starts with an unwavering adoption and dedication to an anti-fraud policy, followed by a fraud risk assessment to determine those areas of the company that are particularly susceptible to fraud. Once that is done, the organization's leadership must put into place those internal controls that will prevent and detect fraud by its employees, continually monitoring them to ensure of their continued effectiveness. While these controls may not prevent all fraud, at least the organization can seek to minimize the effects of such fraud. Utilizing some of the resources mentioned in this paper will hopefully guide management in this quest.

REFERENCES

Association of Certified Fraud Examiners. *Report to the Nations 2018 Global Study on Occupational Fraud and Abuse* (Austin: ACFE, 2018a).

Association of Certified Fraud Examiners. *Fraud Examiners Manual* (Austin: ACFE, 2018b).

Cheng, Q., Goh, B.W., & Kim, J.B., (2018). Internal Control and Operational Efficiency. *Contemporary Accounting Research*, 35, 2, 1102-1139.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise Risk Management Integrated Framework: Executive Summary*. Retrieved from: https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal Control-Integrated Framework Executive Summary.* Retrieved from https://www.coso.org/Pages/ic.aspx.

Lai, Y., Li, H., Lin, H., & Wu, F. (2017). The Influence of Internal Control Weaknesses on Firm Performance. *Journal of Accounting and Finance*, 17(6), 82-95.

Romney M., & Steinbart, B. (2015). *Accounting Information Systems*, (13th ed.). Upper Saddle River, NJ: Pearson.

Srinivasan, R., & Cornelsen, E. (2017). Characteristics of Firms with Material Weaknesses in Internal Control: An Imperical Study. *Journal of Accounting & Finance*, 17(4), 63-73.