

Limit Risk with Internal Fraud Prevention Controls

The National Association of Certified Valuators and Analysts

Learn How to Set up Prevention Systems, Identify Relevant Data Relationships, and Think Outside the Box

There generally are three types of people who commit fraud: die-hard criminals, otherwise honest people who give in to temptation, and otherwise honest people under severe stress. Strong internal control programs can help two of these types from making a catastrophic mistake. Here's how to protect revenue and discourage criminal behavior.

It is a news headline all too familiar. Investors defrauded out of millions by a wealthy financier. Accounting fraud committed at a multi-billion dollar corporation by management. Employee embezzled hundreds of thousands from his company. While the magnitude of fraud involved in the cases that make headlines does not occur at all organizations, all organizations are at risk for fraud.

Inevitably when we read the details of fraud cases that do make headlines, our first instinct is to assign blame. Internal controls were not in place or were not executed properly. The auditors overlooked obvious misstatements. Investors failed to verify key information. While hindsight vision may indeed be 20/20, often there is more than one weak link in fraud cases. All elements of corporate structure play an important role in detecting and preventing fraud. One important, but often overlooked, line of defense to combat the ever-present risk of fraud is that of today's corporate finance professional.

"At one location for a national fast food chain, several managers concocted a scheme to skim money from sales. It was an idea born primarily out of opportunity. They had worked at the company for longer than many other employees and had access privileges in the point of sale system available only to managers."

Skimming Scheme

At one location for a national fast food chain, several managers concocted a scheme to skim money from sales. It was an idea born primarily out of opportunity. They had worked at the company for longer than many other employees and had access privileges in the point of sale system available only to managers. They first "tested" their idea over several months to see if they would be caught. After a customer paid in cash, the valid sale was canceled by the manager and the cash "skimmed" from the register. When, after several months, they realized no one had caught on to the fraudulent transactions, they expanded their scheme to incorporate more elaborate methods of skimming and cash register disbursement fraud. Corporate-level management did not detect the abnormalities generated from the transactions until over a year into the scheme. The company had recently implemented a new "monitoring report" that detailed abnormal transactions at the store level. After running this report for only a few months, the finance team quickly identified the abnormalities occurring at one store location as a red flag. As soon as they investigated further, the scheme of the three individuals involved in the fraud quickly unraveled.

Prevention

If the fast-food company discussed above had identified a need to monitor sales transaction types at the store level sooner, the individuals described above would most likely have been caught much sooner, or, if the employees knew that such a monitoring process was in place, they may not have committed the thefts. My experience has indicated that there are three types of people who commit fraud against their employer. They are (1) die-hard criminals looking for a way to take advantage, (2) otherwise honest people who give

into temptation when confronted with opportunity over and over again, and (3) otherwise honest people who, under severe stress give in and take advantage of an opportunity to gain financial benefit. Internal controls should be designed to prevent any group from defrauding the company. However, in the case of type 2 and 3 employees, effective internal controls can prevent otherwise honest people from making a catastrophic mistake. When employees are aware that monitoring is taking place, even if they do not know exactly how such monitoring is done, there is a significant deterrent effect for those employees who may give in to temptation or stress. Protecting the companies valued employees is as much a part of effective internal controls as protecting the other assets of the company.

The suggestions offered below will help identify important information to focus on when performing a fraud detection analysis. Once specific tests for fraud are identified, it is helpful to develop a list of all fraud detection tests that are performed and include a description of the specific purpose for each test. Not only will this provide a big picture assessment of a finance team's fraud prevention tactics, but it will explicitly describe the purpose of each test. By implementing a few of the suggestions below, finance professionals can help reduce the risk of fraud at their company.

Identify Relevant Relationships within the Data

The median loss due to occupational fraud, or employee theft, is \$175,000, with more than one-quarter involving losses of at least \$1 million. Approximately 88% of these frauds occur via asset misappropriation.¹ Examples of asset misappropriations include skimming, falsifying expense reimbursements or billing, and payroll fraud. These potential fraud schemes can be directly linked to line items in the internal profit and loss statements. By analyzing relationships in the financial data, irregularities and potential fraud can be identified and further investigated. For example, sales dollars per manager could decrease due to skimming schemes perpetrated by one individual. Third-party consultant or contractor costs per month or quarter could increase due to fictitious invoices. Increased travel expenses per employee could indicate an employee is falsifying expense reports. Payroll expenses per location could increase due to the creation of fictitious employees.



As with most elements of income and expenses, there are multiple factors affecting their behavior. Any one comparison does not necessarily tell the full story, but by performing a few periodic tests on some high-risk areas, abnormalities can be identified and investigated. High-risk areas will vary by industry, but below are a few other potential data relationships to monitor for fraudulent activity:

Number or dollar amount of customer discounts per number or dollar amount of sales. Sales per: location, employee, hour or number of transactions. Any expense line item as a percentage of sales; or other relevant factor. Sales per number of transactions.

Think Outside the Box

Often the various divisions at a company can remain isolated from each other. The daily functions of receiving/production, sales/operations, and accounting/finance functions may be separated by more than just an office. These activities are typically scattered across cities and states. Despite the tendency to be disconnected, it is important that financial professionals be in communication with employees in other areas of the business. For example, operations employees understand the inner-workings of the sales process, an area of high risk for fraud. Receiving and production managers know the areas where the potential for asset misappropriation is the greatest.

Meeting with professionals from different areas within the company to discuss the details of their processes and areas of fraud risk can generate ideas for new fraud prevention analyses. Including IT and

database professionals in these discussions as well is also beneficial. These individuals will understand what information is available and how to extract the necessary detail. Often the data is available but, as what happened with the fast food chain, the right data analysis to detect fraud may not be occurring.

Maintain Professional Skepticism

Professional skepticism for a Certified Public Accountant is defined as “an attitude that includes a questioning mind and working practices that encompass a critical assessment of...evidence”.² Identifying potential fraud requires application of skepticism when looking at financial data. However, many accountants have no specific training in fraud investigation and as a result may be ineffective in applying skepticism for the purpose of uncovering potential fraud. Also, when an accountant sees essentially the same types of reports period after period, they may not notice changes that have gradually occurred and which could indicate potentially fraudulent activity. One procedure to address this situation is to consider bringing in an outside consultant, preferably someone who is a Certified Fraud Examiner, to evaluate fraud detection analyses already in place and offer suggestions for new detection methods. Even without bringing in a consultant, finance teams can themselves reevaluate the types of analyses currently employed by an organization and train themselves to constantly reevaluate current financial information with a more critical eye, which can be helpful in fraud detection. Awareness of the potential for fraud is the key to detection.

Auditor partners are required to rotate off client engagements every five years³ in order to help retain the independence and professional skepticism necessary to be effective at their jobs. A similar concept can be applied to the fraud detection analyses performed by finance professionals. Once the analyses related to fraud detection have been created (as described above), the tests can be performed by a different person each month or quarter. Rotating the person who performs the test on a periodic basis will help to retain a fresh perspective of the analysis and the professional skepticism.

A Note for Small Businesses

Many small businesses may not have the data capabilities or information availability for some of the analyses detailed above. However, the role of a financial analysis in these companies should not be discounted. According to the ACFE, median losses due to occupational fraud at businesses with fewer than 100 employees were \$200,000, which was higher than median losses in any other category.⁴ Although the scale of the fraud-prevention techniques may be smaller, the same methods described above apply to small businesses as well.

Basic Principles Fraud prevention is an important responsibility for anyone in charge of monitoring performance, whether in finance, accounting, or other areas of the company. By analyzing relevant relationships within financial data, brainstorming with professionals in other areas of the business on fraud risk analysis, and retaining a level of professional skepticism with financial information, finance professionals can provide a meaningful role in the prevention process. With involvement from all disciplines, perhaps together we can prevent corporate fraud from being the next major news headline.

Joe Epps, CPA/ABV, CFE, CVA, has over 30 years of experience in forensic accounting. His litigation support experience includes contract disputes, anti-trust, economic damages, fraud investigations, business valuation and intellectual property litigation. Joe is currently President of Epps CPA Consulting and teaches a graduate course on Forensic Accounting at Arizona State University. For more information, go to www.eppscpa.com. Christine Tiano is a CPA and CFE and has over five years of experience in accounting, auditing, and finance. She worked with a variety of clients as an auditor at a public accounting firm, and she has also worked in commercial banking finance, where her focus was statistical analysis and internal reporting. She is currently a Senior Associate with Epps CPA Consulting.

¹ Association of Certified Fraud Examiners 2008 Report to the Nation (www.acfe.com)

² AICPA Practice Alert 98-2 (<http://www.aicpa.org/pubs/cpaltr/sep98/suppl/firms.htm>)

³ SEC Final Rule, Strengthening the Commission's Requirements Regarding Auditor Independence

(<http://www.sec.gov/rules/final/33-8183.htm>)

4 Association of Certified Fraud Examiners 2008 Report to the Nation (www.acfe.com)

VN:F [1.9.22_1171]

Please Wait...

Rating: 10.0/**10** (1 vote cast)

Limit Risk with Internal Fraud Prevention Controls, 10.0 out of 10 based on 1 rating