CAIN ELLSWORTH
& COMPANY, LLP
Beyond the Numbers...

Protecting Your Business From Internal Fraud

Occupational fraud is a serious issue for organizations of all sizes and sectors. Yet, it can be challenging to address because it comes from within your organization and is often cloaked in trust and routine, making it hard to spot.

The cost of fraud is high. The median loss per case is $145,000, but the consequences extend beyond financial losses. Fraud can shake the foundation of your company's culture, break down trust, and tarnish your reputation.

In this document, we'll provide you with four specific controls you can implement to help protect your business.

Understand the types of fraud to look for

When it comes to fraud, the best defense is a proactive offense. To truly strengthen your organization's defenses, you first need to understand the various ways fraud can manifest and what to look for. It generally falls into three categories: asset misappropriation, corruption, and financial statement fraud. However, perpetrators rarely limit their schemes to one category. More than a third of cases involve multiple deceptive acts.

Asset misappropriation

Nearly nine out of ten incidents involve asset misappropriation, where an employee steals company resources. This can range from direct theft of cash and skimming to more intricate schemes like submitting fake expenses. It typically takes a company 12 months to detect misappropriation, and median losses hover around $120,000 per case.

Corruption

Corruption usually involves conflicts of interest, bribery, and extortion. Purchasing schemes, invoice kickbacks, and bid rigging are all examples of corruption. Unfortunately, these schemes tend to cause both financial losses and reputational harm.

Financial statement fraud

Although less frequent, financial statement fraud hits the hardest financially. It only accounts for 5% of incidents, but the median losses skyrocket to $767,000. These schemes manipulate financial statements to misrepresent net worth or income, often through fake revenues, hidden expenses, or unrealistic asset values. Perpetrators often do this to meet financial targets, mask the organization's true financial state, or for personal gain.

Notably, these schemes seldom occur in isolation - if someone distorts financial statements, they're likely engaging in other types of fraud as well.

Identify and assess your risk factors

Every organization, regardless of size or industry, has unique vulnerabilities to fraud. To protect your business, you need to identify your risk factors and create targeted measures to minimize those risks.

Consider the size of your business

The scale of your operation plays a role in the type of risks you're most likely to encounter. Small businesses, with limited resources and fewer employees, often lack the checks and balances found in larger organizations. Compared to larger companies, small businesses tend to have a greater risk of skimming and payment tampering.

Large organizations, on the other hand, tend to face more corruption and non-cash asset theft.

Consider industry trends and vulnerabilities

Different industries are predisposed to specific types of fraud. For example, the healthcare and construction sectors often grapple with billing schemes, while manufacturing, warehousing, and retail sectors are more prone to non-cash theft. Awareness of these trends can help tailor your prevention strategies to address the most pressing risks in your industry.

Consider departmental risks

Fraud can originate from any part of an organization, but certain departments are more frequently implicated. Operations, accounting, sales, customer service, and upper management are common fraud hotspots. Median losses for executive-level schemes are more than seven times greater than those carried out by other employees, so it's essential to tighten controls at all levels - especially within departments that handle financial transactions or have access to sensitive information.

Consider behavioral risks

Don't overlook the human element of fraud. More than 8 out of 10 perpetrators display at least one red flag before being caught. Common warning signs include living beyond one's means, financial difficulties, unusually close relationships with vendors or customers, control issues, and a reluctance to take vacations. HR-related red flags like poor performance evaluations and complaints about pay can also signal potential fraud risk.

Implement proactive prevention strategies

When deceptive activities are uncovered passively through police notifications, confessions, or even accidentally, they've likely been happening for years to the tune of hundreds of thousands of dollars. Proactive internal controls are far more efficient at detecting issues early and minimizing losses.

Unfortunately, over half of all fraud stems from either a total lack of internal controls or a failure to enforce existing policies.

According to the Association of Certified Fraud Examiners, organizations that fall victim to these schemes often lack proactive controls like rewards for whistleblowers, job rotation, mandatory vacation policies, surprise audits, data monitoring, fraud risk assessments, dedicated fraud prevention teams, employee support programs, awareness training, independent audit committees, and a formal process for reporting suspicious activities.

Maximize the impact of your internal controls

The vast majority of companies claim to have a Code of Conduct aimed at deterring dishonest activity, but evidence suggests that this does little to actually prevent fraud. Background checks are another common practice that rarely reveal any warning signs. Nine times out of ten, a background check won't reveal any existing red flags because most perpetrators don't have a documented history of related misconduct.

That said, it's important to focus on the prevention measures that have proven effective and provide the greatest return on investment.

The most recent data shows that four specific controls - surprise audits, fraud awareness training, hotlines, and proactive data analysis - had the greatest impact. Yet, it's these very controls that are among the least used.

Surprise audits keep employees on their toes. Randomize the timing and scope of these audits to increase the perceived risk of detection among potential perpetrators.

Have a formal fraud awareness training program to equip your team with the information they need to identify and prevent misappropriation. And train everyone, not just managers. The vast majority of fraud is detected through employee tips, and employees are twice as likely to report suspicious activity when they've had training. A robust training program should clearly communicate the consequences of fraud for the business and employees and explain how to report suspected fraud. It should also be an ongoing training program, not just something you review with new hires.

Be sure to create multiple confidential reporting channels, prioritizing email and web-based forms, as recent data shows they're preferred over phone hotlines. Pair this with comprehensive training for best results.

Finally, keep in mind that most deceptive schemes go undetected for a full year. By using data analysis software regularly, you can detect unusual activity early and minimize losses.

Final Thoughts

Business changes, technology advances, and fraud tactics evolve, so the tools that worked last year might not suffice this year. Reassess your internal controls at least annually to ensure they adapt to the latest challenges and minimize your exposure to risks.

While your team plays a key role in fraud prevention, external experts can offer specialized knowledge and impartial advice. If you'd like a review of your internal controls and tailored guidance, reach out to one of our expert advisors. We can help identify blind spots in your existing controls and offer insights into the latest anti-fraud strategies.

About Cain Ellsworth.

Cain Ellsworth is not all things to all people. Instead, we specialize in serving small to medium businesses in banking, manufacturing, property and casualty insurance, plus a variety of other industries. And we dedicate significant resources to assure that we are well-informed in each of them.

Cain Ellsworth:

Sheldon, IA Office
1008 Third Avenue
PO Box 449
Sheldon, IA 51201

Sioux Falls, SD Office
5130 E 57th Street
Sioux Falls, SD 57108

IA - (712) 324-4614
SD - (605) 610-4611

sdykstra@cainellsworth.com

www.cainellsworth.com