CSO
FROM IDG

Credit: Thinkstock

Fraud prevention: Improving internal controls

Internal fraud controls aren't fire-and-forget. Smart collaboration and ongoing improvement will help keep fraud in check. Here are the basics.

Daniel Draz, M.S., CFE| MAR 28, 2011

There are several keys to effective fraud prevention, but some of the most important tools in the corporate toolbox are strong internal controls. Equally important, though, are the company's attitude towards fraud, internal controls and an ethical organizational culture. While ethical culture is driven by senior management's control environment ("tone at the top"), buy in from

the company's Board of Directors and Audit Committee are also essential in promoting an ethical and transparent environment.

The focus of this article is on strengthening internal controls. According to the Committee of Sponsoring Organizations (COSO),

> Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting and compliance with applicable laws and regulations.

Internal controls should not be thought of as "static." They are a dynamic and fluid set of tools that evolve over time as the business, technology and fraud environment changes in response to competition, industry practices, legislation, regulation and current economic conditions.

While no company, even with the strongest internal controls, is immune from fraud, strengthening internal control policies, processes and procedures definitely makes companies a less attractive target to both internal and external criminals seeking to exploit internal control weaknesses.

Strengthening internal controls is seldom accomplished by enhancing one process; rather it involves a comprehensive review of the risks faced, the existing internal controls already in place and their adequacy in preventing fraud from occurring. An internal control review may be conducted corporate-wide or on a location by location basis, or broken down to the individual business unit level. Generally, a review of this nature involves an in depth examination of people, processes and technology. However, there are other intangibles your organization cannot afford to overlook.

Audit interaction

The first part of strengthening internal controls involves changing the attitude some employees have towards auditors. While it is easy to view auditors as the police department's "Internal Affairs" group — whose sole responsibility it is to ferret out wrongdoing, identifying employees who are breaking the rules — personal and professional success is to be had by viewing auditors as key partners and allies in the battle against fraud. This is further reinforced as the auditor's role ensures that he or she is always at the forefront of corporate policies, practices, procedures, technology, new products and services, making auditors a valuable source of corporate information.

Secondly, part of strengthening internal controls is simply a matter of defining, or clarifying, ownership roles and responsibilities.

A common misperception among corporate employees is that internal controls are solely the responsibility of the company's Audit Department. While internal auditors measure the effectiveness of internal control through their efforts, they don't generally assume ownership.

They assess whether the controls are properly designed, implemented and working effectively and make recommendations on how to improve internal control.

According to the Institute of Internal Auditors (IIA), "responsibility for the system of internal control within a typical organization is a shared responsibility among all the executives, with leadership normally provided by the CFO."

Companies with strong internal controls (policies, processes and procedures) view the process holistically and find a team approach valuable. An effective team environment encompasses members from a variety of different business units and disciplines and may include representatives from: Human Resources, Compliance, Investigations, Audit, General Counsel's Office, Senior Management, and Security (Information and Physical).

Strengthening internal controls is seldom accomplished by enhancing one process; rather it involves a comprehensive review of the risks faced, the existing internal controls already in place and their adequacy in preventing fraud from occurring.

To manage the process effectively, individual departments work together in an interactive manner. Working together increases issue awareness, strengthens communication, reduces opportunity for fraud and ensures a more comprehensive and robust internal control process.

Failure to work together may have consequences as indicated by this example:

A finance company utilizing more of an individually owned internal control process discovered an employee theft. Before making other key stakeholders aware of the theft, the department immediately acted on the information and confronted the suspect employee. While the employee ultimately admitted to the theft as was known at the time, the failure to bring other departments into the equation had significant long term impact. Post-investigation research and forensic analysis ultimately determined that the employee was part of an organized ring. Not only were funds stolen, but so was personally identifiable information (PII) which may have been used to commit identity theft outside the corporation. While the investigation should have been driven exclusively by the investigations department, the magnitude and scope of the operation would have been identified earlier had the appropriate individuals been involved at the outset of the incident under a uniform internal control group with clear lines of responsibility and authority.

So, the question is: what are the best practices used to get people to cooperate in a group like this? While it would be easy to say that there's a best practice standard for getting different managers, executives and business unit leaders to the table to agree on internal control protocols, ownership and responsibilities, unfortunately given the differing cultures and operating dynamics in each company, there isn't a "one size fits all" solution that is going to work uniformly for every company.

However, from my experience, a "top down" approach involves the formation of an internal controls working group, headed by the audit department with the support of the audit committee. This works in many companies, especially as there is accountability under Sarbanes Oxley to the audit committee and the company's board of directors. While some business unit leaders naturally resent being told what to do, what processes to implement, and how to implement them, eventually most will comply given the regulatory and internal reporting environment mandating that certain steps are taken. It is possible to avoid the resentment through good old fashioned relationship-building, where you bring multidisciplinary teams together willingly under the auspices of tightening internal controls and building a stronger company.

Communication

One way to strengthen internal controls is by improving the communication process. I've seen countless situations where key stakeholders are unaware of major events occurring within a corporation or business unit. This is problematic as there is no opportunity for management to fix something that they're unaware is broken. Regular interaction and communication between departments is paramount in this process.

Communication protocols must be established and agreed upon enterprise wide. Critical incident event distribution notification processes and procedures must be in place to ensure everyone is aware of an incident and understands what their defined roles are when the incident occurs.

An effective notification system operates over a central server, delivers event messaging to predefined employees in "real time," as the event occurs, and is sent directly to the employees and their smart devices.

Part of incident awareness lies with the ethics, hotline and event notification systems being used by the corporation pursuant to Sarbanes Oxley requirements. Many industry professionals have experience with the operation of ethics and compliance hotline systems but not all incidents are reported through these compliance mechanisms. One of the key questions surrounds how companies notify key stake holders when an event occurs outside the ethics or compliance system? While this communication often falls under a first responder type program, it is imperative that companies have defined processes and communication protocols in place to notify the key management employees who "need to know."

An effective notification system operates over a central server, delivers event messaging to predefined employees in "real time," as the event occurs, and is sent directly to the employees and their smart devices. This level of event notification ensures that the people who need to know about an incident are made aware in a timely manner and fosters immediate and unified response as required.

While many companies either utilize in-house resources or contract with a vendor to provide these ethics, code of conduct and incident reporting services, an increased number of system reports generally assist in strengthening internal controls as it provides more opportunities to evaluate reported events and corresponding internal control deficiencies.

One of the methods to strengthen the internal controls associated with this process involves evaluation of the communication protocols used to promote the ethics hotline, employees awareness of the hotline tool, how to access it and ways to use it effectively. According to the 2010 ACFE Report to the Nation, frauds are most likely to be detected through a tip than by any other means. This process may be strengthened through increased promotion of the hotline in company mailings, internal communications, newsletters and company website.

While not all calls to the ethics hotline are indicative of an internal control weakness or fraud, the ones that are demand increased scrutiny to determine root cause analysis. Once the root cause has been determined, there is an opportunity to strengthen internal controls if a control was either exploited or nonexistent.

Segregation of duties

One area where many companies can significantly strengthen their internal controls involves segregation of duty policies and this is often considered the "primary internal control." It is imperative that there are adequate segregation of duties involving custody, authorization and control of source documents and records. That is, one person should not have the sole authority to initiate a transaction, authorize or approve a transaction and complete the transaction without appropriate sign off processes and differing levels of management approval. The lack of proper segregation of duty policies is most often the root cause of many fraud and theft events in companies without strong internal controls in this area.

One area where many companies can significantly strengthen their internal controls involves segregation of duty policies and this is often considered the "primary internal control."

There have been so many examples of fraud committed directly as a result of a company's failure to segregate duties that it's not necessary to focus solely on one. Rather, it's important to examine the common themes that contribute to these frauds. The fraud usually occurs in a finance area; involves someone with unsupervised control over company funds and documents (checks) and access to banking accounts for deposits and withdraws; there is no segregation of duties and the fraud occurs in companies with lax internal controls. So, for example a bookkeeper is able to write a check to himself without worrying about being detected.

Using established fraud prevention best practices, financial duties (cash disbursements) should always be segregated amongst multiple employees. This usually means that there are multiple employees involved in the financial process with oversight at several places in the process. This ensures that one employee cannot manipulate the entire process and increases awareness

amongst employees that someone is not only looking, but conducting random audits to reconcile financial transactions. Check stock should be controlled and secured, secondary levels of management approval and dual signatures on checks and payment authorization on amounts over pre-established financial levels should be required. Further, all employee should have individual financial transactional levels established which vary according to their management levels, or position of authority, business unit needs and ability to obligate the business to a financial commitment.

Checks are not the only area of concern. The same type of internal controls should be in place for company credit cards and electronic payment tools. It would be just as easy for one employee with complete responsibility for accounts payable to fraudulently wire money outside the company or establish fraudulent electronic payments without the proper level of oversight and control. Segregation of duties in this area would also prevent an employee from creating "phantom" vendor accounts, false invoices and making payments against those invoices without additional verifications in place.

Lessons learned

While no company wants to experience internal or external fraud events, victimization may have long term corporate anti-fraud benefits if all departments have comprehensive incident handling protocols and the incident is handled appropriately after the fact.

Appropriate handling always includes post event analysis which provides the company with an excellent "lessons learned" opportunity. During this process stakeholders need to be asking the tough questions and gathering information to identify the factors that allowed the event to occur.

The process should not be viewed as a fault finding mission but a determination of whether there was a company, policy, procedure or guideline in place to address this situation, whether the guidelines were followed as designed or adequate to address (or prevent) the specific situation that occurred.

If the fraud event occurred because an employee(s) simply failed to follow the internal control policies, then there are corrective measures that business units may take to ensure policies are followed in the future. These include communication to employees regarding increased awareness, correct handling processes and policy adherence. It may simply be that employees performed as expected under the circumstances but there were insufficient internal control policies in place to guide their behavior. Lessons learned here will strengthen internal controls through the creation of new ones.

A fraud event without in-depth incident evaluation, lessons learned and corrective action generally means that there is an excellent chance the criminals will reload the activity and the company will continue to experience high levels of fraud.

A great example of this involves timekeeping amongst non-exempt employees. Many companies are now using electronic payroll systems offered through services like ADP to track arrival at work, departure from work, lunch, sick and vacation days. The systems work well but like any

other technology, after implementation, there are always employees trying to figure out how to beat the system and steal time. Simply put, arrive 15 minutes late to work and your check is being docked that amount of time. Once two or three investigations are conducted into this kind of activity the methods used by employees trying to manipulate the clock are known and the holes that allowed the activity to occur can be plugged. Additionally, as stealing time is usually a violation of the company's Code of Conduct policies, when employees are terminated for stealing time, and it becomes known that termination is what the company's response to that action was, it serves as a deterrent to future activity like this.

Technology

While technology enables us to perform essential business functions, there are direct correlations between technology, fraud events and the internal control process. Technological applications are probably the single greatest sources of risk and exposure that businesses face. Robust internal controls, including platform and network access controls, remote usage and password protection policies, are needed to regulate the entire computing platform.

Additionally, there must be internal controls in place for all mobile computing applications and company telecommunication devices like personal computers and smart phones. Given how quickly technology is changing, strengthening internal controls in this area revolves around fluid processes as the technology is not static.

A great example of the evolving technology, risk and demand for internal controls involves cloud computing. While cloud computing is viewed as a way to reduce computing costs, the need for strengthened internal controls is significant as your company's information is not under your direct oversight and control.

As indicated earlier, this is a significant reason why information security professionals are one of the teams responsible for internal control oversight.

Fraud risk assessments

In accordance with current legislation and regulation, many of the internal controls in place today are specifically designed to protect Personally Identifier Information (PII), and consumer data in the possession of businesses. In today's business environment, consumer and information protection are paramount. Internal controls can be strengthened through departmental fraud risk assessments, audits, and an examination of policies and procedures, particularly those that involve employees who have direct interaction with consumers and their PII. The methods in which data's gathered, handled, stored, and destroyed in conjunction with the company's data retention practices should be examined in detail. Additionally, an assessment of the information and physical security practices, protection methods and controls surrounding the consumers and their PII data should be conducted to find the vulnerabilities and take corrective actions surrounding these internal controls.

Providing self-assessment check lists to department managers and requiring a semi-annual review of policies, practices and procedures is an effective method for assessing key controls and

ensuring that they are adequate for preventing fraud. Additionally, fraud risk assessments safeguard company assets, protecting the company from added liability and financial exposure. Oversight for semi-annual review usually comes from either the compliance or audit departments. While PII is a major concern for privacy reasons and data breaches, there are a variety of critical business processes and procedures that could be examined in fraud risk assessments depending on the type of business, the industry and the regulation or oversight of the business. Oversight for fraud risk assessments is typically the responsibility of the company's audit department.

Providing self-assessment check lists to department managers and requiring a semi-annual review of policies, practices and procedures is an effective method for assessing key controls and ensuring that they are adequate for preventing fraud.

Testing key controls

It is essential to differentiate fraud risk assessments from control testing. The primary purpose of fraud risk assessments is gathering information about processes, procedures and controls while control testing determines whether the controls are working as intended or not.

It is important that we test internal controls in a controlled environment as internal controls that are only tested under "live fire," real time conditions may not actually be effective controls at all. Testing is an integral part in any control environment and may be a key indicator in not only assessing how strong the internal controls are but whether they need to be strengthened. Simulated, situational testing may also assess event readiness and effective business unit processes. The type of testing, the regularity of the testing and the testing schedule will vary from business to business and may be determined by individual company needs and regulatory requirements.

All technology and information based tools should be tested. A perfect example of internal control testing in the technology area involves testing access controls and information availability via online Internet information platforms. A recent test conducted by one company found a security flaw in the platform, which unknowingly exposed consumers' PII to the general public and had been doing so for a period of years until it was detected. The hole was plugged but the damage was already done!

According to the SEC, Section 404 of the Sarbanes Oxley Act requires and reinforces the need for control testing:

> The Act directs the Commission to adopt rules requiring each annual report of a company, other than a registered investment company, to contain (1) a statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) management's assessment, as of the end of the company's most recent

fiscal year, of the effectiveness of the company's internal control structure and procedures for financial reporting. Section 404 also requires the company's auditor to attest to, and report on management's assessment of the effectiveness of the company's internal controls and procedures for financial reporting in accordance with standards established by the Public Company Accounting Oversight Board.

Conclusion

In this article, we've discussed a number of methods and approaches for strengthening internal controls. One thing is certain: Given the ever changing business and regulatory environment and the number and diversity of types of frauds being committed against companies globally, internal controls must be reviewed, evaluated, tested and strengthened regularly.

It's insufficient to create internal controls and expect them to stand the test of time without periodically modifying them to meet current conditions.

Daniel W. Draz, M.S., CFE is the Principal of Fraud Solutions, a specialized corporate fraud and investigation consulting firm. He has a Masters degree in Economic Crime Management and 26 years of sophisticated fraud, investigation, compliance, audit and risk experience exclusively in the private sector. Contact him via e-mail: info@fraudsolutions.com.