

Anti-fraud measures aren't one size fits all*

Originally published in the Volume 56 . 2008
issue of Growing Your Business™ magazine

All businesses need to protect revenue and reputation from the potentially devastating effects of fraud. PricewaterhouseCoopers' Biennial Global Economic Crime Survey found that companies with both ethical guidelines and compliance programs report suffering fewer acts of fraud and other crimes.

However, as businesses change, reach across geographic boundaries or their employees become determined to outwit internal controls, management must review fraud-risk management programs to ensure they remain effective. Employees trained to spot fraud, deter and prevent it can be powerful allies. Featured is an eight-step program for fraud-risk assessment.

Protecting your financial health and reputation

Every business needs to protect its financial health and reputation from the potentially devastating consequences of fraud and other forms of misconduct. And, according to PricewaterhouseCoopers' fourth biennial Global Economic Crime Survey released in 2007, "Economic Crime: People, Culture and Controls," many businesses could be doing a better job of guarding their money, property or legal rights. More than half of the 500 US companies surveyed report having been affected by economic crime. Crime, such as fraud, not only could cost in terms of revenue, it could also harm a company's reputation and even cause its collapse.

Though companies are likely to have at least some level of controls in place, and procedures to minimize fraud risk, they are still subject to fraud if controls are inadequate or become so as businesses change or employees learn to work around procedures. And private companies, which typically are less likely than their public counterparts to have effective anti-fraud programs and controls, can be reluctant to report and prosecute fraud for fear of adverse publicity.

"A challenge, for many private companies is working out how to strike the right balance between having *enough* trust in employees so they can thrive and having *too much* trust, which would provide opportunities for fraud," observes Jeff Able, a PricewaterhouseCoopers' Private Company Services partner.

The extent of activities required to evaluate fraud risks at a company should be commensurate with the size and complexity of its operations and financial reporting environment. Such risk assessment efforts are proving worthwhile. The 2007 Survey found that companies with both ethical guidelines and compliance programs reported suffering fewer economic crimes.

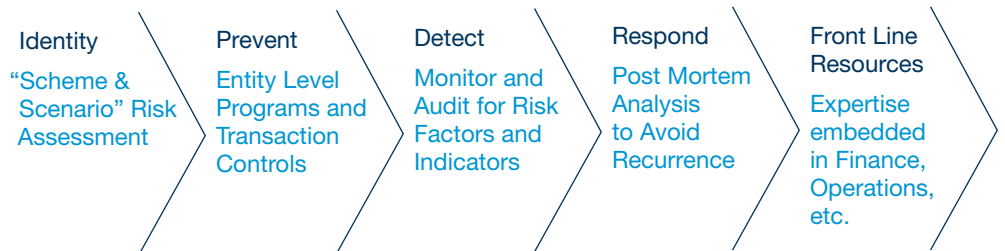
A detailed focus on improving business controls has the added benefit of potentially improving the company's operating effectiveness and stopping revenue leakages, such as providing services below normal pricing, failing to use proper pricing codes and offering credit to unqualified customers. Businesses could be better able to fight fraud by educating employees on how to help prevent, deter and detect it. "Employees are the eyes and ears of private business," says Bill Warren, a director of fraud risk and controls with PricewaterhouseCoopers' Advisory Services group. "If something is amiss, they are likely to know about it before management or the company's auditors."

Focus on the transaction level

While the Global Economic Crime Survey found that the level of damage appears to be directly proportional to the seniority of the perpetrator, fraud at this level occurred in only about 29 percent of the companies surveyed. This underscores how important it is to go beyond entity-level anti-fraud controls and set priorities for addressing possible issues at the business process or transaction level. The foundation of fraud prevention is the division of responsibilities between employees. The reason is straightforward: It is one thing to steal by yourself but quite another to collude with a coworker.

Often, private companies say they lack sufficient personnel for an efficient checks and balances system. However, a simple step, such as ensuring that the same employee who approves vendors doesn't have the authority to write checks, can help reduce fraud risk. The close-knit company that believes fraud "can't happen here" and allows the same employee to approve vendors, sign checks and reconcile the bank statement and keep its books is an easy target.

What practical steps might a company take to defend against internal and external misconduct?



How well does the company unlock company information to identify what could go wrong?

How well does the company leverage risk assessment process to reinforce local accountability?

How efficient is the assessment process, e.g., are the businesses asked to do more than one assessment?

How well does the company address vulnerability to management override of controls, collusion among employees and/or third parties, or other forms of collusion when designing preventive controls?

How well does the company tailor detection procedures to key risk factors and indicators?

How well does the company maximize existing information systems to prevent and detect misconduct?

How well does the company learn lessons when misconduct is detected? Does it analyze root cause, extend audit procedures to root out other misconduct?

How well does the company embed fraud and misconduct expertise at the "front line"—does it over rely upon the "second line", e.g., compliance, ethics, internal audit, legal?

Not only must businesses have preventive measures in place, it is essential that they continue monitoring them for effectiveness. “Companies without internal audit departments, or personnel serving in that capacity generally lack a process for periodically determining if the anti-fraud controls management believes to be in place are designed appropriately or operating effectively,” Able notes.

Many fraud risks and the opportunity for misconduct differ from company to company and industry to industry and need to be considered when developing internal controls. For example, a business in the construction industry would be expected to have controls in place to prevent employees from bribing public officials to win large contracts. Not only does bribing a government official for a contract risk prosecution of both individual and employer by the US Department of Justice, if it takes place overseas, it is also subject to the Foreign Corrupt Practices Act and the foreign country’s local laws. On the other hand, retailers and consumer products manufacturers must guard against damage to their brand and reputation. The loss of consumer confidence related to a fraud incident can be devastating.

Where to begin

A sound risk management program not only takes into account industry-specific issues, but is also designed in light of the company’s current operations and longer-term strategy.

First, a company must review its compensation programs and performance evaluation process to identify potential incentives and excessive performance pressure such that employees resort to fraud to make their numbers. This review considers how meeting—or not meeting—financial reporting targets potentially impacts an individual’s evaluation, compensation and continued employment.

Then, management conducts a fraud risk assessment to identify various other ways that fraud and misconduct can occur throughout an organization. It sets priorities for addressing areas subject to a higher risk of fraud. [See Eight-Step Program for Fraud Risk Assessment on page 6.]

While evaluating and testing the design and operating effectiveness of entity-wide anti-fraud controls, there’s no substitute for thinking like a fraud perpetrator seeking to override them. A very good summary of what private companies should consider when developing a fraud-risk management program, the “COSO: Guidance for Smaller Companies Principle 10—Fraud Risk,” was created by the Committee of Sponsoring Organizations of the Treadway Commission.

Watch out for new risks

As a business grows and adds new locations and new vendor relationships, someone independent of the day-to-day operations should reassess controls in place to ensure they are still designed and operating effectively, revisiting questions such as: Can someone set up a fictitious vendor? Does the person who reconciles cash accounts also have access to the general ledger? And, other key questions targeted to the business. In emerging markets, the 2007 Survey found that 61 percent of parent companies that employed different accounting systems than those of their subsidiaries, reported they were more susceptible to fraud, compared to 52 percent that operated a unified system.

Two faces of fraud

You might think of fraud as actions that cost an organization directly, such as embezzlement, accepting bribes or kickbacks or intentionally concealing or misrepresenting events, transactions or data. However, fraud can be designed seemingly to benefit an organization for the direct or indirect benefit of the perpetrator, such as to gain a management bonus or promotion.

According to guidance strongly recommended by the Institute of Internal Auditors, *Practice Advisory 1210.A2-1: Auditor’s Responsibilities Relating to Fraud Risk Assessment, Prevention, and Detection*, examples of fraud designed to benefit the organization include:

Improper payments, such as illegal political contributions, bribes, and kickbacks, as well as payoffs to government officials, intermediaries of government officials, customers, or suppliers.

Intentional and improper representation or valuation of transactions, assets, liabilities and income, among others.

Intentional and improper transfer pricing (e.g., valuation of goods exchanged between related organizations). By purposely structuring pricing techniques improperly, management can improve their operating results to the detriment of the other organization.

Intentional failure to record or disclose significant information accurately or completely, which may present an enhanced picture of the organization to outside parties.

Sale or assignment of fictitious or misrepresented assets.

Intentional failure to act in circumstances where action is required by the company or by law.

Intentional errors in tax compliance activities to reduce taxes owed.

Prohibited business activities, such as those that violate government statutes, rules, regulations or contracts.

Any business reaching across borders for clients, acquisitions, suppliers and investors, must monitor its internal controls to maintain integrity in the face of different cultures and legal environments. And, like US laws, the laws in other countries are subject to change. “In recent years, several large companies have had significant compliance issues because they were not keeping up with the changing laws,” observes Warren.

In the grand scheme of day-to-day business, how important is appropriate fraud-risk management? Is it worth the time and expense to ensure that an employee cannot misappropriate as little as \$400 without calling attention to it? “It depends,” says Warren. “If that employee is using the \$400 to bribe a foreign official to win a contract it could cost the company far more in fines, penalties and investigative costs.”

Don’t underestimate the power of a tip hotline, even if it’s just an e-mail address. The most common way that 60 percent of the businesses in the 2007 Survey say they discovered fraud within their organizations was by accident, or a tip from another employee.

While it may not be possible to eliminate the risk of fraud altogether, with proper planning, policies and procedures, and controls in place, your company can minimize the risk of serious fraud, and at least detect fraudulent activity early and minimize its damage. A comprehensive fraud risk management program also should include an incident response and remediation process to address allegations or suspicions of fraud or misconduct.

An 8 step program for fraud-risk assessment

- 1 Assemble a fraud-risk assessment team. Make sure the team is broad and deep enough. For example, a vice president of one business area might understand a risk in theory, but someone on the factory floor is more likely to better understand how things are actually processed.
- 2 Decide on scope, framework and deliverable. Are you interested in financial statement manipulation, asset misappropriation or other criminal activity? At what level does it become material to the company? How detailed should controls be? How are you going to gather information, rate your risks and map risks to controls within your organization?
- 3 Identify inherent risks. Consider risks without regard to existing controls to avoid relying upon ineffective or inefficient controls.
- 4 Assess likelihood and significance of risks. Significance depends upon the nature of the risk, e.g., a potential fraud scheme may be inconsequential to the financial statements, but very significant to the company’s operations.
- 5 Link significant risks to transaction controls and evaluate the controls. Don’t overlook design effectiveness—a control may be adequate to protect error, but vulnerable to override, collusion or other intentional circumvention.

Want to know more about creating a robust fraud-risk management program? Please contact:

Jeff Able
Partner, Private Company Services
678-419-3121, jeffrey.l.able@us.pwc.com

Jonny Frank
Principal, Advisory Services
646-471-8590, jonny.frank@us.pwc.com

Bill Warren
Director, Advisory Services
678-419-1574, bill.warren@us.pwc.com

Or visit our website at www.pwc.com/pcs to locate the PricewaterhouseCoopers office nearest you.

by independent feature writer Janice K. Mandel,
mandel.schneider@erols.com

Need additional guidance?

The following publications provide greater detail on creating and maintaining effective internal controls to prevent fraud and other significant risks in the financial reporting area.

Coso: Guidance for Smaller Companies Principle 10—Fraud Risk

2007 SEC Guidance Regarding Management's Report on Internal Controls over Financial Reporting

IIA Practice Advisory 1210.A2-1: Fraud Risk Assessment, Prevention & Detection

Statement on Auditing Standards No. 99 Consideration of Fraud in a Financial Statement Audit

6 Share residual risks with business unit and process leaders. Because business leaders are accountable for misconduct in their unit or process, provide them an opportunity to decide which risks for which they accept responsibility (non-residual risk) and those for which they are unwilling to accept accountability—because a preventive control is deficient or not practical.

7 Develop remediation plan, for example, proactive anti-fraud audit procedures to address risks when red flags occur. Require the business leaders, working with finance, to develop a remediation plan to reduce risk to an acceptable level by either enhancing preventive controls or focusing on early detection.

8 Perform fraud auditing and monitoring as needed. Re-engineer the risk to identify potential red flags. Design auditing and monitoring procedures to detect and follow up on key risk indicators.

Does your fraud-risk management program pass the test?

Evaluate your fraud-risk management savvy using the Anti-fraud Program and Controls Assessment Grid at www.pwc.com/gyb

pwc.com/pcs

This document is provided by PricewaterhouseCoopers LLP for general guidance only, and does not constitute the provision of legal advice, accounting services, investment advice, written tax advice under Circular 230 or professional advice of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisers. Before making any decision or taking any action, you should consult with a professional adviser who has been provided with all pertinent facts relevant to your particular situation. The information is provided 'as is' with no assurance or guarantee of completeness, accuracy, or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties or performance, merchantability, and fitness for a particular purpose.

PricewaterhouseCoopers' Private Company Services practice is an integrated team of audit, tax and advisory professionals who focus on the unique needs of private companies and their owners. Within the practice, our professionals concentrate on the needs of manufacturing, retail, wholesale and distribution, construction, and food and beverage companies, as well as on the needs of law firms and other professional service organizations. They are committed to delivering cost-effective, practical solutions and proactive services with the quality clients expect from PricewaterhouseCoopers.

© 2008 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. *connectedthinking is trademark of PricewaterhouseCoopers LLP (US).