Fraud in an economic upturn

Managing the downside of an upswing

July, 2011

A review of how fraud and other integrity risks affect business.

At a glance

Those charged with governance should take the lead in demonstrating that fraud and integrity are critical business issues—not just legal and compliance issues.

The implementation of anti-fraud and other compliance program elements typically lag the pursuit of sales opportunities as programs may lose valuable resources allocations after a downturn.

Recent US legislation increases the likelihood of external reporting of allegations of misconduct, raising the stakes for those charged with governance.

pwc

Is the very nature of fraud, corruption, abuse and other integrity threats changing amid the economic recovery? And if so, how? Read on as we look ahead to highlight the issues that boards of directors and audit committees need to prepare for: the frauds that might emerge and the likely regulatory response to them. And we describe the strategies that proactive organizations are implementing to manage short-term risks and enhance stakeholder value over time.

Fraud and integrity risks

Incentive and pressure

In this time of increasing economic growth, individuals and organizations are more aggressively seeking opportunities to successfully compete in a global economy.

The strategies are many: from expanding operations through mergers and acquisitions to tapping new customers, business partners, and products, and boosting the bottom line by embracing cost-saving strategies such as outsourcing and technological solutions.

While misconduct can, from a legal perspective, be perpetrated by a company, the steps taken to commit fraud are always the actions of individuals. It's sometimes assumed that people commit fraud for personal gain, particularly to obtain money. People are said, for example, to "cook the books" in order to earn a large year-end bonus, but the reality is far more complex. While personal financial gain is often a factor, in other instances, the principal motivation might be personal reputation, pressure from above, or a desire to help the organization succeed.

As the economy begins to recover, pressure grows to increase revenues, net profits and otherwise enhance performance metrics. The need to meet or exceed expectations is an incentive that might lead individuals to cast aside internal control activities and enter into riskier transactions. Additionally, during a period of growth, organizations are competing to quickly grab their share of emerging—and limited—opportunities while there's still time to secure a piece of the action.

At the same time, recovery means rebuilding and expansion for many organizations. Companies will hire new people or rehire those let go during the downturn. Both populations might face increased pressures to commit fraud if they've been out of work for any length of time. In the case of new hires, for example, a lack of familiarity with controls can reduce the effectiveness of those controls.

New business opportunities can also introduce new business partners, including new vendors, joint venture partners and acquired companies. Insufficient due diligence over vendors can expose entities to risk of vendor and procurement fraud. Similarly, lack of analysis of prior acts and reputations of acquired companies can result in overpayment for assets and successor liability for those prior acts.

Opportunity

It's axiomatic that change is the only constant. But we now see that economic growth is accelerating the rate of change.

Expansion might outpace the resources needed to manage growth, including additional employees, internal controls and systems enhancements. In our experience, the implementation of anti-fraud and other compliance program elements typically lags the pursuit and expansion of sales opportunities, particularly after a downturn, when the programs may have lost valuable resource allocations. Organizations seeking growth opportunities in new industries, products, and international markets, including in emerging regions, might also face new regulatory challenges, local laws and customs.

As the economy improves, vigilant enforcement of internal controls can weaken as long as revenues and profits are on the rise. Although organizations might monitor expenses (disbursement of assets) more closely than they did before the recession, the motivation to effectively perform this task might diminish. Petty frauds such as employees overstating business-related expenses or office supply theft are more likely to be overlooked when times are good.

Considering the recent spate of Ponzi scheme scandals, companies should also be on the lookout for investment opportunities that appear too good to be true, for they usually are just that. In times of economic growth, it's possible that susceptibility to such scams might be greater as people seek greater returns on investment and are willing to take risks they might not normally take.

Even as the US and global economies improve, fraud risks pose new threats: thefts of electronic data and physical assets, insider trading scandals and financial mismanagement, corruption and bribery, procurement fraud, and regulatory and compliance violations.

Rationalization

During a period of economic revitalization ripe with new opportunities and business strategies, the capacity for people to rationalize fraud and corruption both changes and increases. The third element of the fraud triangle is the ability of individuals, be they front-line operations staff or members of the board of directors, to rationalize the fraudulent act.

To illustrate what we mean by this, here are some examples of rationalization, with a particular emphasis on themes that are almost certain to emerge in this period of growth and recovery:

- Everyone pays bribes to make sales in that country; there is no other way.
- Cooking the books or "creative accounting" is not fraud; it's just bending the rules.
- I'm the only one left in my department after redundancies. I have to do all the work and haven't had a raise in two years. I deserve the money!
- It's not a big deal if I lie about meeting this quarter's earnings targets. I'm too embarrassed to admit the truth to sub-par performance.[1]
- I didn't seek out material non-public information. Rather, I came into possession of it through my position, and being an opportunist, I used that information to trade.[2]
- No one will notice if I take this inventory item.
- It's not a lot of money compared to how much this company earns.
- I'll return the money next month.
- We need this contract to meet our sales goal and I'm going to do whatever it takes to get it.
- I receive a commission for my sales.
- I sell investments to clients without disclosing to them certain information that would lead a reasonable investor to determine that the product is not suitable for them. However, they do receive some benefit and I don't want to lose a sale. What they don't know won't hurt them.[3]
- Computers store large amounts of data in one place, and the complex technology leaves room for error. Finding a way to access and use this information is an easy way to make money and gain fame.

We know it's likely that economic growth following a severe downturn can increase fraud risk. We also know that frauds last a median of 18 months before being detected and thus bad behavior that occurred during the downturn is likely to be detected about now.[4] But what are the implications for corporations, investors, regulators and the government? Here are the questions we believe boards and audit committees should be asking themselves and their pivotal stakeholders:

In the wake of cost containment measures undertaken during the recent financial crisis, what is the status of enterprise-wide fraud risk controls and related compliance programs? Are they robust and modern enough to detect and prevent fraud?

We continue to be amazed at the paltry number of organizations that truly understand what fraud is actually costing their business. It remains relatively rare for companies to have proper insight into the various fraud risks they face, or to have appropriate controls designed and implemented to address these risks.

Fraud losses will continue to run at high levels, with some commentators putting the estimate of losses from fraud at 5% of revenue.[5] While this may appear high, we see continuing opportunity for significant fraud losses as many organizations continue to underestimate and under-respond to avoidable fraud losses by failing to develop adequate controls, especially with respect to growth initiatives such as mergers and acquisitions or expansion into emerging markets. This trend will likely continue as

1. http://www.sec.gov/news/speech/2008/spch090909lar.htm, *Why Does Fraud Occur and What Can Deter or Prevent it?*, by Lori Richards
2. Ibid.
3. Ibid.

long as organizations treat anti-fraud programs as an obstacle to, rather than an enabler of, good business.

Internal audit departments have also been depleted as a result of the economic downturn. And as a result, potential wrongdoers might see an opportunity to get away with fraud.

Proactive risk management is good for business.

Is your organization at risk of DOJ, SEC, or foreign government scrutiny?

The Department of Justice (DOJ) and Securities and Exchange Commission (SEC) continue to clamp down hard on corruption. Other governments around the world are also beginning to implement more powerful laws, such as the UK Bribery Act, which went into effect July 1, 2011.

While many companies have taken steps to create the right global anti-corruption policies, too few have put the right processes and controls in place to prevent corruption. At the same time, the sophistication of those who are accepting bribes has evolved. The Fraud Triangle is complete: Significant opportunity remains within some global organizations to engage in bribery (via 'consulting' payments or benefits in kind) while incentive (to win new business or match competitors' success) and the ability to rationalize (it's 'market practice') also remain high.

Scandals during the recession also created conditions for heightened government scrutiny beyond the realm of corruption. Primary factors include increased regulation and greater government involvement in many aspects of economic life. In the US, the Dodd-Frank act alone generated a wide variety of new reporting requirements and incentives for whistleblowers to report to the government perceived wrongdoing.

In addition, various governmental stimulus packages, inside and outside the United States, increased government participation in companies and industries that heretofore had been unregulated or more lightly regulated. Regulators are themselves also under pressure, as some perceive them to have been ineffective in anticipating or preventing recent financial scandals. While these factors don't necessarily directly increase the risk of fraud, they do increase the likelihood of governmental scrutiny over recipients of government 'bailout' money and industries thought to have been at the heart of the financial crisis.

How well does your organization know the people with whom it does business?

Organizations are increasingly being held accountable for the actions of agents, suppliers, and other counter-parties. Regulators are prosecuting companies and their directors and officers for the inappropriate actions of business partners such as distributors and sales agents. Companies shouldn't simply ignore the actions of business partners who might be willing to pay bribes to achieve sales, but many still do.

Risks lie not just in the sales channel but also in the supply chain. Organizations in many industries have suffered reputational, legal, and financial loss due to fraudulently concealed unethical practices arising in the supply chain, including:

- Agents paying commercial and public bribes
- Suppliers failing to pay rebates
- Sub-contractors sourcing materials from non-sustainable sources

Organizations also face several varieties of fraud risk from new joint venture partners, such as asset misappropriation and unwitting violation of US regulations such as export controls laws, with which partners might be unfamiliar.

Some—but not all—organizations are beginning to address these risks by using techniques akin to investigative journalism to conduct integrity diligence on business partners.

We see continuing high levels of motivation and opportunity for this type of fraud in the race to win market share. To limit legal, financial, and reputational risk, organizations should

4. Association of Certified Fraud Examiners 2010 Report to the Nation on Occupational Fraud and Abuse.
5. Ibid.

consider implementing appropriate due diligence and monitoring controls with respect to their business partners. The clear rationalization in these instances is that, "I can't control the actions of my business partners," when, in fact, organizations can and do exert a fair amount of influence over them.

Is your organization at risk of a significant data theft?

In the past, discussions about fraud, integrity, and asset losses have tended to focus on cash, tangible assets (e.g. stock/inventory), and financial securities. In 2009 and 2010, the losses of electronic personal data experienced by public and private sector organizations were widely reported.

Criminal organizations have for some time recognized the value of personal data and as long as bank account and credit card details continue to have a black market value, a significant risk of theft will remain.

We see opportunity as the principal threat resulting from the inadequacy of data privacy controls. In our experience, many organizations have begun to make basic arrangements to improve privacy and data security. However, most of these improvements require continuous monitoring and investment, something that companies might have put off during the recent economic crisis. Furthermore, many organizations allocate resources to the threat of external data breaches when, in fact, most data theft occurs internally. Organizations should assess their electronic data safeguards and related controls to address the risk of accidental loss or deliberate theft.

Is your organization at risk in the way it recruits and trains new employees?

Companies will hire new people or rehire people let go during the downturn. Bringing on new employees during an economic upturn, unless carefully planned and managed, skyrockets internal and external misconduct risks. As noted earlier, both populations might have increased pressures to commit fraud if they've been out of work for any length of time. Amid the frenzy of 'government bailouts' and the general public backlash against big business, they might rationalize ill-gotten gains as entitlements. Making matter worse, when organizations rush to get recruits through the door, they risk inadequately training new hires, who then fail to understand policies, procedures, and controls, which undermines the effectiveness of those controls.

In short, the economic upturn will, for some individuals, increase the motivation and ability to rationalize misconduct. We also foresee increasing opportunity as back-office headcount is increased.

How strong is your first line of defense?

Operations and finance personnel comprise the first line of defense against fraud, corruption, and abuse. While they play a critical role, most compliance, internal audit, and legal departments are one step, if not two or three, removed from the day-to-day business. As a result, it's not wise to rely exclusively on them as the principal line of defense.

We've observed that organizations that viewed misconduct management as a 'discretionary spend' during the economic downturn are retreating from efforts to equip front-line personnel with antifraud knowledge, skills, and tools. They need to demonstrate that they have taken reasonable steps to guard against fraud, corruption, waste, and abuse and can expect little sympathy from regulators, investors, journalists, and overseers when misconduct occurs, especially when it could have been prevented or more quickly detected if front-line personnel were more fraud savvy.

How reliable is your financial data?

Fraud can be difficult to identify when senior managers have colluded with third parties to misrepresent financial information and statements. Audit committees should consider whether any aspects of the company's control

environment have been compromised as a result of actions taken during the recent economic crisis and pose some crucial questions:

- How strong is the ethical tone at the top and in the middle?
- Are duties and responsibilities adequately segregated?
- Are remuneration systems promoting the right behaviors?
- Is the segregation of key duties and responsibilities still adequate following any cost-cutting initiatives?
- Do we have an adequate whistleblower hotline and would employees speak up if they had concerns?
- How well resourced is internal audit, compliance, and other third lines of defense?
- Does internal audit have the necessary fraud detection experience?
- Do our international operations have adequately staffed and competent finance departments?

If a crisis occurred, how well prepared are you to react?

We expect the DOJ and SEC to continue to adopt more proactive approaches to the detection and investigation of fraud and regulatory breaches. Prosecutors and regulators expect organizations to implement effective controls over criminal conduct just as public companies must have effective controls over financial reporting. The government expects—and, for government contractors, requires—that the company:

- Identify and assess criminal conduct risk
- Evaluate design and validate operating effectiveness or preventive and detective controls
- Conduct monitoring and auditing to detect criminal conduct

Companies must report, at an early stage, when a regulatory breach, fraud, or corruption is identified. Those that fail to do so and eventually get found out receive harsher sanctions and, if a government contractor, face potential suspension or disbarment from doing business with the government.

Companies need to be "investigation ready," meaning they will need to have policies in place regarding the conduct of investigations and will be expected to know where data is stored and how it can be speedily retrieved. Companies must also demonstrate that they have taken action to prevent recurrence, beginning with ring-fencing the issues to understand whether the perpetrators engaged in other, unrelated wrongdoing or whether similar misconduct occurred elsewhere in the organization. The organization needs to conduct root-cause analysis: Did the misconduct result from a poor control environment, inadequate risk assessment, poor preventive controls and/or weak detection processes?

In addition to criminal prosecutions, regulators are making more use of their ability to seek civil penalties to dispose of some cases. In seeking to resolve investigations in this way, regulators will take into account:

- The steps taken before the incident to identify the risk, develop controls, and conduct auditing to detect misconduct
- The rigor with which an organization reacted to an alleged incident, including the thoroughness and independence of any internal investigation
- The quality and comprehensiveness of the organization's efforts to conduct a root cause analysis and implement and monitor controls to prevent recurrence
- The cooperation afforded them by the company

Given the heightened regulatory environment, companies should have appropriate contingency plans in place to enable them to react and respond immediately to a fraud or regulatory crisis. We have noted several instances in which those organizations that are prepared when these situations arise have been able to limit the economic cost and the duration of the matter.

Each organization must determine how best to implement a fraud and integrity risk strategy. We set out below some of the questions those charged with governance need to ask and get answered to gain comfort that a sound strategy is in place.

The strategy of the proactive organization

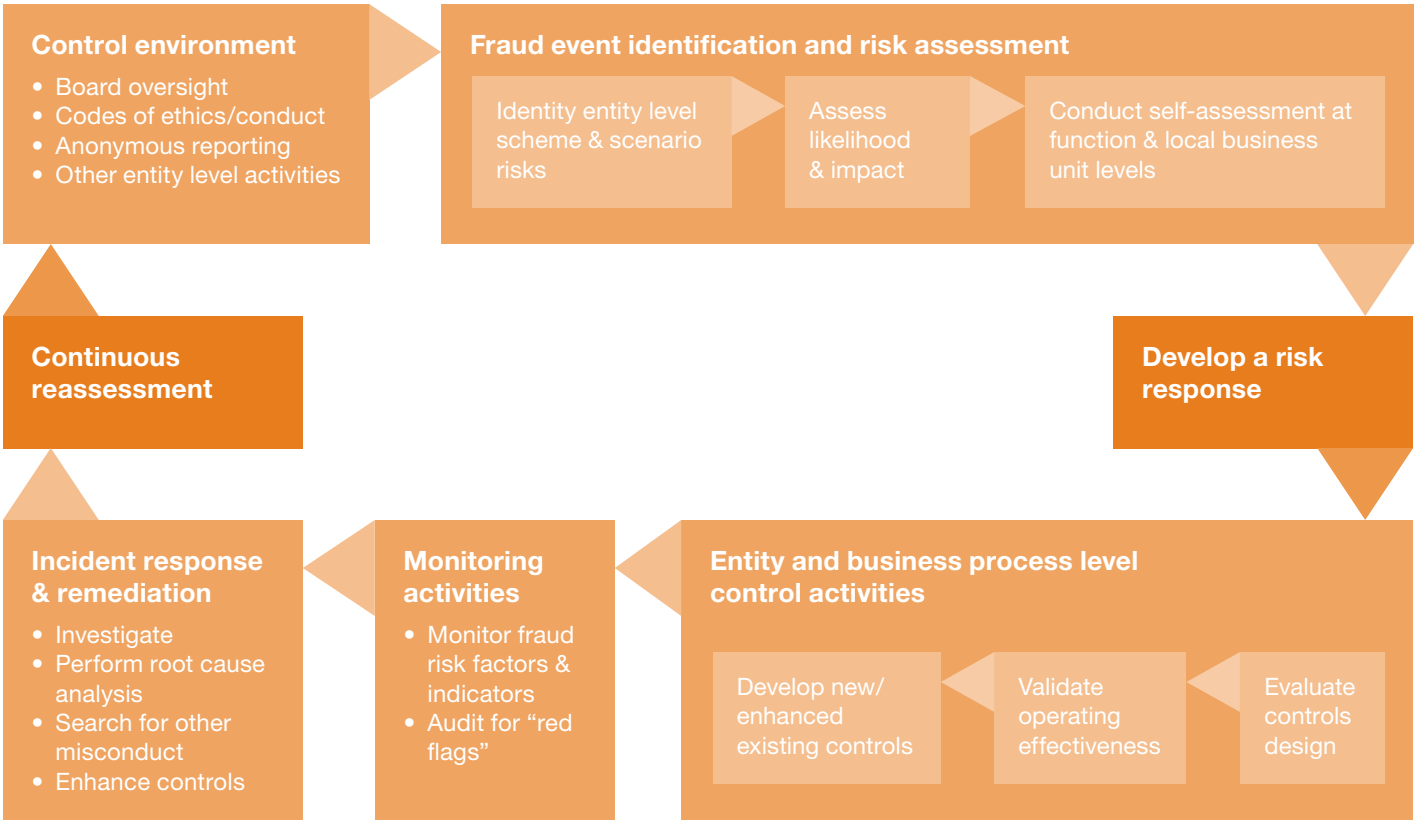

Figure 1: The PwC antifraud framework

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed a model for evaluating internal controls. This model has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control. We have adapted the COSO framework to illustrate some of the key elements of a fraud and integrity risk control framework.

Organizational tone

What steps are being taken to be certain that the right tone at the top permeates down through the organization?

Does our remuneration strategy, including bonus arrangements, support or undermine the organization's ethical stance?

Management information

Does middle and senior management have the knowledge, skills, and tools they need to manage fraud and integrity risks?

Communication and training

Do our people receive proper communication and training?

Are operational and finance staff an effective first line of defense against fraud and integrity risks?

Risk identification

How does management identify fraud and misconduct risk?

Who is making this assessment and what information is the assessment based on?

What input is received from the business unit and functional leaders who serve as the first line of defense?

Has anyone thought through the fraud and integrity risks arising from the people we do business with, including our sales agents, distributors, joint venture partners, and supply chain?

Control linkage and evaluation

Is the control system designed principally to identify errors or is it sufficiently robust to prevent or detect fraud, corruption or other misconduct risks?

Monitoring activities

Has the organization identified key risk factors and indicators?

What process do management and internal audit use to identify key risk factors and indicators?

Incident response & remediation

Are we conducting thorough, independent investigations?

How well do we analyze the root cause of misconduct and enhance/monitor controls to prevent recurrence?

The economic upturn is changing the nature and scale of fraud and integrity risks that organizations are up against. The speed of change is such that opportunities to commit fraud will be prevalent. Although those charged with governance are grappling with many competing priorities, in our view boards of directors would be wise to reflect carefully on the changing landscape of fraud and other integrity risks.

Turning up the heat on fraud

Those charged with governance should take the lead in demonstrating that fraud and integrity are critical business issues—not just legal and compliance issues. Employees look to the board and senior management to set the tone and unless senior-level commitment is apparent, the organization will not see the right kind of change, nor will it realize the benefits of reducing fraud and other integrity risks.

The good news is that effective fraud risk management more than pays for itself. Companies across industry sectors are desperate to find ways to reduce cost. Attacking fraud, waste and abuse offers a huge cost savings opportunity for a relatively low investment.

The challenge organizations face is that there is no single 'key' to stopping fraud and misconduct. Organizations need to develop a strategy that enables the deployment of appropriate measures to manage this increasing risk. The strategy needs to be owned by front-line personnel; otherwise it will not succeed. Most large organizations have mature legal, compliance, and internal audit functions. But these are one step removed from where the fraud and misconduct occur. Front-line operations and finance personnel need to become effective first and second lines of defense.

PwC has developed a self-assessment tool that enables organizations to benchmark their fraud and integrity risk program. Please contact the author of this white paper if you would like to know more about how we can help you manage these challenges.

About PwC forensic services

Fraud prevention and detection experience

Fraud specialists face the daunting task of discovering misconduct in the absence of an allegation. Just as doctors need medical manuals, fraud specialists require knowledge of the various ways that misconduct is committed, prevented and detected. PwC has invested over 100,000 hours researching common, sector- and market-specific misconduct schemes involving fraudulent reporting, asset misappropriation, and criminal conduct. PwC risks and controls professionals developed manuals detailing the mechanics, controls, risk indicators and detection procedures for hundreds of fraud scenarios, which are tailored to specific client needs and circumstances.

Thought leadership

PwC is a thought leader in prevention, investigation and remediation of fraud. Hundreds of companies have used our anti-fraud framework—which has been embraced by COSO, SEC, IIA, and the AICPA—to benchmark the effectiveness of efforts to guard against misconduct. We have published numerous fraud prevention whitepapers, beginning with the seminal Key Elements of Anti-fraud Programs and Controls published in 2003 and continuing with industry specific guides. Related publications include Confronting Corruption*, The Business Case For An Effective Anti-Corruption Programme, and PwC's Biennial Global Economic Crime Survey.

Global reach and trustworthy brand

PricewaterhouseCoopers (www.pwc.com), provides industry-focused assurance, tax and advisory services to build public trust and enhance value for its clients and their stakeholders. More than 155,000 people in 153 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

Contact information

Contact us

San Francisco
Kristin Rivera
kristin.d.rivera@us.pwc.com
(415) 498-6531

New York
Dhaval Sheth
dhaval.k.sheth@us.pwc.com
(646) 471-8552

Washington
Neil Keenan
neil.keenan@us.pwc.com
(703) 918-1216

Peter Viksuins
peter.viksnins@us.pwc.com
(703) 918-1514

www.pwc.com