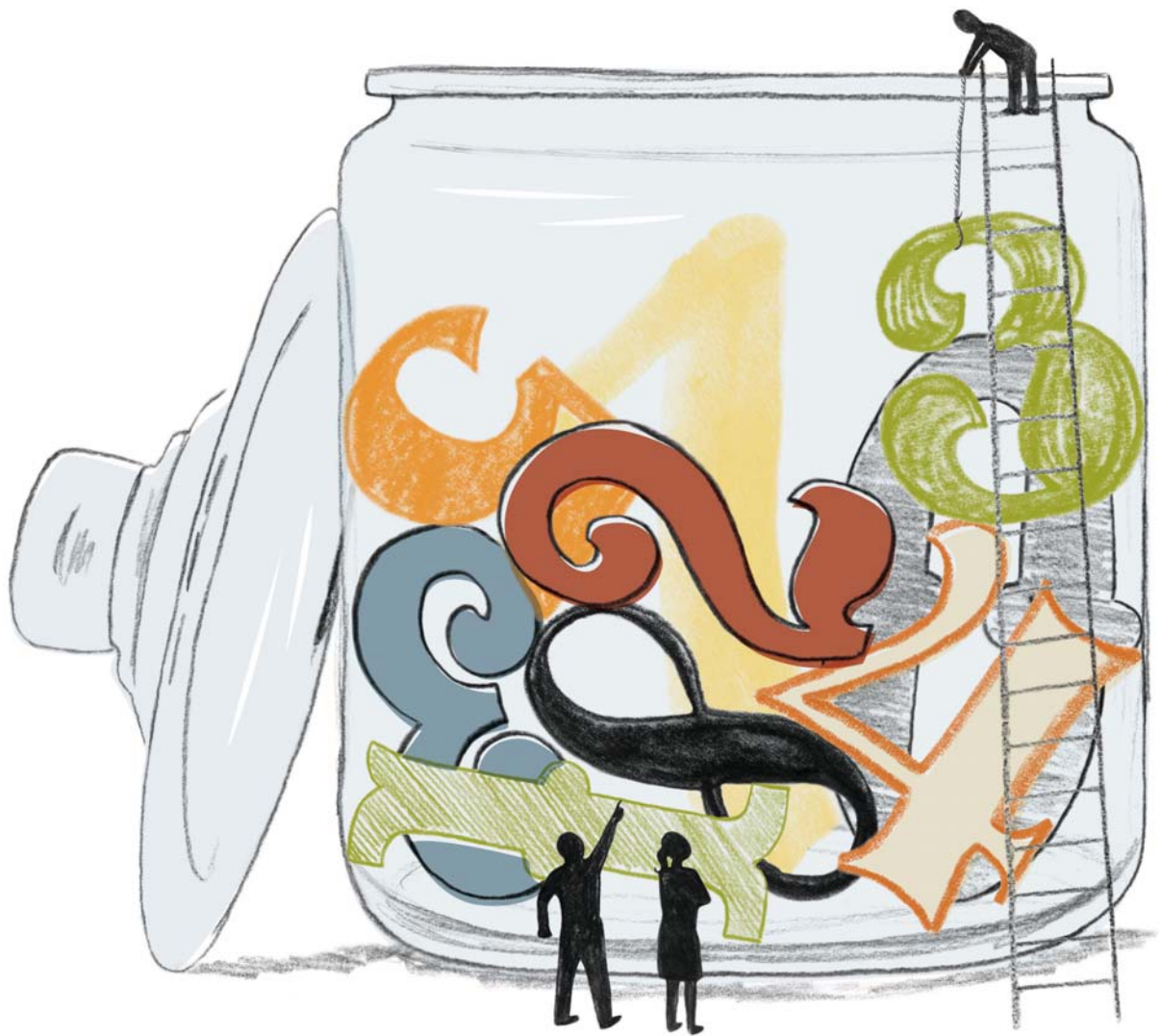


*CorporateGovernor* series:

# Fraud in the economic recovery

---

Addressing the concerns of the Corporate Governance Community Spring 2010





## Contents

- 1 Introduction
- 2 Private sector fraud
- 4 Government-related fraud
- 6 Preventing fraud
- 10 Conclusion
- 11 About the authors
- 12 Resources

# Introduction

Last year's recession ground economic activity to a halt, but recovery, although currently slow and uneven, is taking hold. Companies that want to capitalize on an improving economy must position themselves for renewed growth, especially if they wish to take advantage of opportunities arising from the continued flow of federal economic stimulus funds. In addition, companies can benefit from the strategic and financial opportunities that come from merging with or acquiring some of the struggling businesses and distressed assets available in the marketplace.

But renewed growth and business activity can also throw less beneficial activities into the mix, increasing the risk of fraud. Of course, fraud is nothing new. It has undoubtedly been around since the first marketplace was established, and it takes many forms. Given the depth and severity of the recession and the pace of the current recovery, with some industries and geographic regions improving more quickly than others, it should come as no surprise that fraud risk remains a pressing concern.

It would be ironic indeed if a company that has made it through a crippling recession should be damaged by recovery-enabled fraud. No one is looking. Economic conditions are improving. More money is coming into the company. Some might wonder, "Why not take some?" When an organization is receiving stimulus money, the potential for fraud may be even easier to rationalize: "After all, the federal government is giving out more than \$700 billion. Who is going to miss a few dollars?"

Fraud in today's environment can be large- or small-scale, committed against the government or private enterprise. To avoid these scenarios and make the most of government and private sector opportunities, executives must evaluate how well their organizations are equipped to prevent, identify and eliminate fraudulent activity. This means assessing the strength and effectiveness of policies and procedures, due diligence approaches, and the internal control environment. It is also critical to react quickly if fraud does occur.

This paper discusses the key issues organizations face when it comes to identifying, dealing with, and protecting themselves from two important types of fraud: fraud committed by or against a private enterprise and fraud committed by entities against the federal government.



# Private sector fraud

Corporations face very specific fraud risks in this recovery, both inside and outside the organization.

## Internal risks

The internal risk of fraud has increased, largely because the economy remains in upheaval. The global economy may be emerging from the deepest recession in recent memory, but the scars remain. This recession has created more chaos, greater displacement and more problems than many anticipated.

True, the stock market is on the rise, but high unemployment levels linger and overall job security remains low. Executives of struggling companies are often desperate to keep their companies afloat. Employees who are angry, afraid and insecure because of the recession's financial impact on friends, family, colleagues and themselves could be tempted to do things they never would have considered before. As a result, the current environment invites an increased potential for internal fraud at exactly the time when many companies' ability to identify and combat fraud has been compromised.

According to a 2009 survey of 729 senior executives conducted by risk consulting firm Kroll Inc.<sup>1</sup> and published in its 2009/2010 *Global Fraud Report*, 30 percent of responding executives report increased levels of fraud at their organizations as a result of the recession. One in six of those surveyed say that their companies are more vulnerable to fraud because of cutbacks in internal controls, and one in seven say increased fraud is the result of employees receiving few or no pay increases.

As the survey indicates, weakened internal controls are a major concern in this environment. When companies downsized to reduce costs, finance, internal audit, loss prevention and other departments responsible for implementing or monitoring internal controls received no reprieve from the cost-cutting ax. Among the staff that remained, many were reassigned from internal control responsibilities to more pressing priorities. Others no longer have enough time or resources to do as thorough a job on internal control management and monitoring as they did in the past.

## External opportunities and risks

Fraud can also result from the actions and decisions of executives trying to improve company performance as the broader economy recovers. The fundamental changes to the economy that occurred during the recession — particularly in industries such as construction, real estate and financial services — have left many executives worried about their companies' prospects for the future. The recession and the credit crisis created serious debt and cash flow problems that some companies have been unable to overcome.

Many of these struggling companies are looking for a buyer or merger partner as they attempt to maximize what, if any, value remains of their companies and avoid a more dire solution such as bankruptcy. In such cases, positioning a company for an acquisition, merger, or sale to a private equity firm or strategic acquirer may be the only way for the organization to survive.

---

<sup>1</sup> *Global Fraud Report*, Annual Edition 2009/2010, Kroll Inc., New York, N.Y., pg. 6, [www.kroll.com/include/document.aspx?file=/library/fraud/FraudReport\\_English-US\\_Oct09.pdf](http://www.kroll.com/include/document.aspx?file=/library/fraud/FraudReport_English-US_Oct09.pdf)

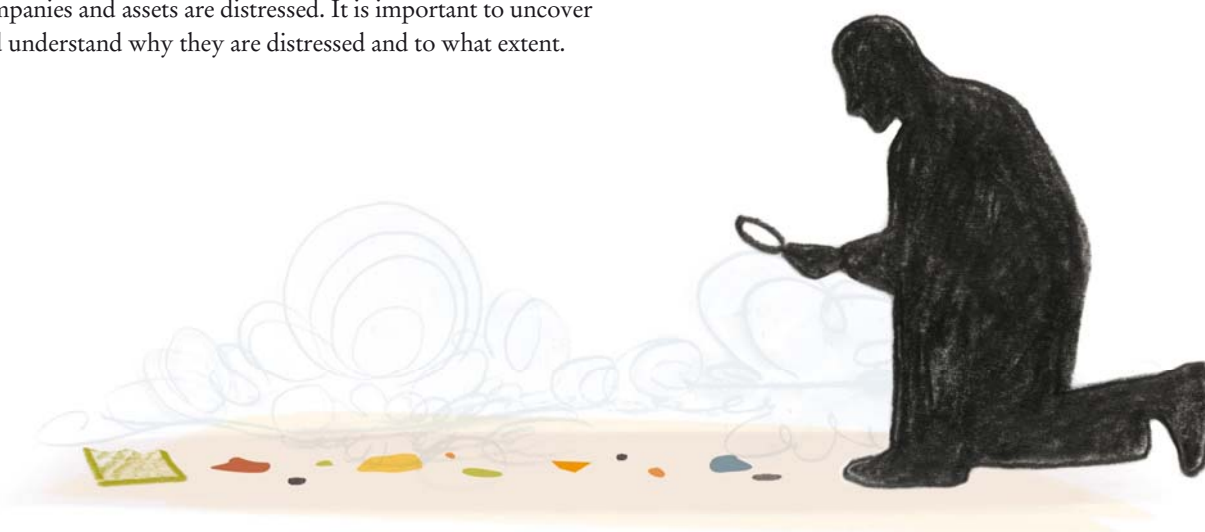
Meanwhile, many companies that had been sitting on cash reserves throughout the recession are now looking to acquisitions for strategic advantage or quick economic gains. Savvy executives see opportunities for strategic acquisitions at prices that are a fraction of what they were just a few years ago. However, the business owners and management teams of target companies and owners of distressed assets could be motivated to act inappropriately — including not making proper disclosures and even actively hiding problems from prospective buyers — in order to make these companies more attractive to potential buyers and maximize prices.

In this environment, “caveat emptor” (Latin for “let the buyer beware”) is definitely the watchword. Executives need to maintain clear heads and resist calls for a quick deal. With bargains to be had, owners and executives of cash-rich companies are champing at the bit to do some bargain shopping and may be tempted to forgo comprehensive due diligence in order to take advantage of this buyer’s market. As a result, they could find that an acquisition can quickly become more of a problem than an opportunity. There are reasons these companies and assets are distressed. It is important to uncover and understand why they are distressed and to what extent.

### The need for vigilance

Even when recovery is taking hold, fraud can still take a toll on an organization. Therefore, constant vigilance and quick action are necessary. After all, fraud committed against a company just emerging from recessionary times can have a sizable impact on long-term performance and overall viability.

When the economy is growing, companies are often making enough money and have ample access to capital and credit; they are therefore in a better position to withstand any fraud that does occur. Early in a recovery, the fallout from fraud is likely to be felt sooner and have a greater impact on the company and its future prospects than it would have at a later date. This makes preventing private sector fraud more important than ever. Above all, the governance and integrity of an organization that is the victim of fraud may be called into question by means of shareholder lawsuits, and the board may be held liable should it fail to maintain vigilance and safeguard the company sufficiently.



# Government-related fraud

Given the amount of government money flowing into the economy, it is fairly safe to assume that fraud against the government will increase. Most government fraud is committed by individual citizens. Last year, in one jurisdiction alone, prosecution of more than 400 cases of fraud involving food stamps, Medicare and unemployment payments resulted in nearly \$2 million in restitution.<sup>2</sup>

Other types of fraud are more complex and are committed by private sector organizations that are recipients of federal funds through the Troubled Asset Relief Program (TARP) — the economic stimulus program funded through the American Recovery and Reinvestment Act of 2009 (ARRA) — or through routine government contracting. The potential fallout from one rogue business unit, executive or employee committing fraud against the government can be significant, both financially and reputationally. For example, in March 2009, Daewoo Engineering and Construction Co. Ltd. had to pay the federal government more than \$50 million in penalties after submitting a fraudulent claim involving a road project on the island of Palau.<sup>3</sup>

The scope of the federal stimulus initiative means that many companies are likely to gain business from some aspect of the program. According to Grant Thornton LLP's 15<sup>th</sup> *Annual Government Contractor Industry Survey*, 37 percent of respondents expected modest or significant revenue increases from contracts funded by the economic stimulus outlined in the ARRA. However, designating money to set up internal controls is not necessarily an attractive option for contractors that are working with finite resources to achieve the often incompatible goals of competing for contracts and turning a profit.<sup>4</sup>

## A systemic problem?

Fraud involving government funds has always been an unfortunate fact of life, and many times the government itself unintentionally is partly to blame. We've all heard of the inflated charges to the government for routine items and wondered how this could possibly happen. In response to such criticisms, federal, state and local governments are getting better at ferreting out fraud and are investing heavily in fraud detection. Despite this commitment to reducing fraud and increasing the transparency of funding, governments will always have the challenge of combating an enormous number of potentially fraudulent activities. Indeed, in some instances, the chances of getting caught are slim; yet being the target of a government fraud investigation is hardly desirable.

In years past, the government paid out funds but did not set up robust enough controls to monitor and oversee the programs it funded. Lack of a fraud prevention infrastructure and generally poor accountability for fraud prevention within agencies added to the problem.

Even government officials do not really know how much fraud is occurring, and quantifying it would be a monumental task that would itself require significant government funding. While there is a strong desire to eliminate fraud from government programs, the success of anti-fraud efforts has yet to be determined because these programs are the biggest targets of all for fraudsters.

No government program has been exempt from fraud, but some cases are more egregious than others. Indeed, programs with the most urgency are often the ones that suffer the greatest amount of fraud — mainly because there is no time to set up robust controls, or because the controls that are in place are circumvented or ignored in the face of that very urgency. A report issued by the U.S. Government Accountability Office in June 2006 estimated that 16 percent of payments, or about

<sup>2</sup> "Welfare Fraud Cases Increase: Unemployment, Recession Believed to be Factors," KPRC Local 2, Feb. 24, 2010, [www.click2houston.com/news](http://www.click2houston.com/news)

<sup>3</sup> [www.ca9c.uscourts.gov/opinions/07-5129.pdf](http://www.ca9c.uscourts.gov/opinions/07-5129.pdf)

<sup>4</sup> Grant Thornton LLP's 15<sup>th</sup> *Annual Government Contractor Industry Survey*, [www.GrantThornton.com/govconSurvey](http://www.GrantThornton.com/govconSurvey)

\$1 billion in individual assistance funds, awarded following Hurricanes Katrina and Rita were fraudulent.<sup>5</sup> Fraud of this magnitude was possible largely because controls designed to verify the appropriateness of payments were relaxed or forgone entirely in order to deliver relief to affected individuals as quickly as possible.

While faster delivery of relief funds is a laudable goal, it is difficult to reconcile the loss of 16 percent of disaster relief funds in the pursuit of that goal. Anyone concerned about federal spending and the national debt must be concerned about fraud in government spending. From a taxpayer's perspective, any dollars lost to fraud add to existing debt without doing anything to provide desperately needed services.

But the government cannot defeat fraud on its own. Companies that receive federal funds through any of these programs also have an important role to play. These types of situations, and ongoing evidence of fraud among some government contractors, highlight the need for more effective internal controls both within government and among recipients of government funds.

### **Recipients, police thyselfs**

The relative paucity of government fraud prevention and oversight often means that contractors and other recipients of federal funds are expected to police themselves. For example, there has long been significant fraud in the delivery of health care through Medicare and other federal programs. However, because fraud detection resources are so limited, it could be years before a government audit uncovers that fraud. In the meantime, significant resources have been either lost or diverted from their primary purpose of service delivery.

These circumstances make it alarmingly easy for perpetrators to avoid detection. Many individuals who commit this type of fraud do so because government funds represent easy money and the risk of being caught is relatively low compared with other

types of financial crime. Billing for nonexistent Medicare services is easier and less risky than robbing a bank and often requires only a laptop computer and a bit of ingenuity.

More recently, the federal government, which has always talked about transparency and accountability in federal spending, seems to have put its money where its mouth is in the case of economic stimulus funds distributed under the ARRA and via other federal spending programs. The Fraud Enforcement and Recovery Act of 2009 (FERA) increases both the federal government's power to investigate and prosecute fraud perpetrated against it and the funds allocated for financial fraud enforcement.

In addition, the Recovery Accountability and Transparency Board was created by the ARRA to investigate and prevent fraud. This board must report quarterly to Congress on its progress. Individual citizens can report potentially fraudulent activity through toll-free phone and fax numbers, the mail, or an online complaint form at [www.recovery.gov](http://www.recovery.gov).

Identifying fraud within TARP can be particularly difficult because there is little to no data or tracking information on how the money was spent. Nevertheless, the Special Inspector General for TARP (SIGTARP) is still investigating and prosecuting fraud. Through the end of 2009, SIGTARP reported 77 ongoing criminal and civil investigations into TARP, accounting, bank and mortgage fraud, among other areas.

Although these fraud prevention efforts on the part of federal government are good signs, more work needs to be done. The passage of FERA and the effectiveness of the Recovery Accountability and Transparency Board and SIGTARP can still be hampered by the relative lack of data available and difficulties in generating that data in the near future.

That is why recipients of federal funds still have a significant role to play in overall fraud prevention and detection. By effectively policing themselves, companies can ensure that they are protecting both themselves and their federal agency clients.

---

<sup>5</sup> Report #GAO-06-844T, [www.gao.gov/new.items/d06844t.pdf](http://www.gao.gov/new.items/d06844t.pdf)

# Preventing fraud

The best tools for combating fraud are effective due diligence and internal controls. By strengthening and enhancing due diligence processes and internal control activities, companies can avoid taking on fraud-related problems when acquiring a new business or merging with another company, and they can identify and prevent problems within existing operations.

## Due diligence

Effective due diligence is always a critical component of a successful merger or acquisition. However, companies that do not want to fall prey to fraud in today's environment need to be more vigilant than ever about the due diligence process. The executives at a target company have a lot of incentive to present that company in the best light possible in order to strike the best deal. Even if the management team of a potential target company is not committing outright fraud, there is still the chance that a more passive type of fraud is present, such as information not being reported correctly or in full.



The right acquisition can be worth a great deal more than the price paid. However, if a company is not careful with its due diligence, the wrong acquisition can create a lot of problems. Savvy stakeholders, including the board of directors and lenders, need to scrutinize their due diligence process closely to make sure it passes muster. In a seller's market, the sellers dictate the terms and speed at which the due diligence process occurs. However, in today's environment it is the buyers who are more in control, and sophisticated buyers demand a thorough due diligence process.

Rather than changing their due diligence methodology or tactics, companies should focus on ensuring that due diligence reaches more broadly and deeply into the target company. It is important for acquirers to have wide-ranging discussions with the target company's management in order to gain a better understanding of the specific risk factors affecting its product, technology and reputation.

For example, because the federal government is taking a strong tack on enforcing laws such as the Foreign Corrupt Practices Act (FCPA), due diligence should include questions and information gathering that can uncover evidence of any violation. The U.S. Department of Justice recently confirmed that they currently have more than 140 open FCPA investigations.<sup>6</sup> In January 2010, 22 representatives of companies in the defense and law enforcement equipment industry were arrested at a Las Vegas trade show for FCPA violations. These arrests are notable for their number and because federal law enforcement officials targeted individuals rather than a specific corporate entity. Moreover, the public nature of these arrests was meant to send a message to individuals and companies that the government is serious about FCPA enforcement.

<sup>6</sup> Lanny A. Breuer, Assistant Attorney General, Criminal Division; remarks made at an FCPA undercover operation press briefing, Jan. 19, 2010. See [www.justice.gov/criminal/pr/speeches-testimony/documents/01-19-10AAG-remarks-FCPAenandpad\\_0.pdf](http://www.justice.gov/criminal/pr/speeches-testimony/documents/01-19-10AAG-remarks-FCPAenandpad_0.pdf)

### Covering all the bases

No two acquisitions are the same. The due diligence required for a bankruptcy-related sale — in terms of how the process will unfold and when and how it will be handled — will be completely different from what would be required for a company undergoing a more moderate form of distress. Therefore, it is important to understand the dynamics of the deal that is being proposed and the fundamental operations of the target business.

### Operational due diligence

Due diligence means not only diving deeper to gain a better understanding of the company's dynamics, financial information and operational data, but also looking at all important aspects of the business. If you wish to identify odd or questionable patterns in any part of a company, it is a good idea to involve staff or service providers in operations, HR and other functional areas. One can discover many issues by walking through a plant and talking to people on the shop floor. No one is more capable of holding these conversations and identifying potential fraud than people who work in operations. In addition, the due diligence team needs to verify the reliability of the data being provided.

### Risk due diligence

Risk due diligence focuses on potential regulatory compliance and legal issues. If a company acquires a business in another country and the acquired entity's executives and employees are involved in bribing government officials in that country, the acquirer could end up with significant legal problems due to FCPA violations or violations of other laws or regulations. The same issue arises for a U.S. company that acquires another U.S. company with foreign operations. In this case, the risk may be even higher, because the acquirer may be more complacent about its due diligence when the target company is based in the United States. Therefore, companies need to be aware of FCPA noncompliance risks both for their overseas operations and for

agents acting on their behalf in other countries. The government will take a much more positive view of a company that has a violation if management did a good job of trying to identify issues during the due diligence phase. If they didn't bother to look, their claim that it was an acquisition and they didn't know won't carry much weight these days.

### Investigative and reputational due diligence

Due diligence is not designed to uncover fraud. Indeed, it is unlikely in and of itself to detect fraud. However, buyers can and should scrutinize management teams and other key players involved with the target company. Such investigative due diligence can be as important as financial due diligence.

Because fraud often starts at the top, buyers should perform background checks on a target's management team, owners and other key players. If any of these individuals have a prior history of involvement in questionable activities — from criminal activities to fraud to past affiliations with other struggling companies — that history could be a warning sign to look closely at what is going on in the target company. For example, an investigation might uncover executives' propensity to extract the value from a company before selling what remains. If members of the target company's management team sold another company 10 years ago, it is important for the acquirer to look at how that company has fared since then.

### Controls environment analysis

In addition to conducting normal financial due diligence, the investigative team should scrutinize the target's internal controls closely. In the day-to-day control environment, there should be a strong segregation of duties, with appropriate internal controls that are handled by two parties and reported to an independent organization such as an external auditor. It is also important to review those operating and control matters involving the IT environment that could have a direct bearing on the deal's financials.

### Internal controls

Effective internal controls are important for every company, whether that company is in the midst of a merger or an acquisition, receiving government contract monies or other funds, or simply operating as normal. The key is to develop an internal control structure that is robust and flexible enough to be modified and updated easily as a company's activities and circumstances change. There are many tools including those used by the internal audit function that can help an organization improve its internal control environment.

### Tone at the top

The tone for the overall business should be set through ethical behavior at the top, including management's adherence to stated company standards and values. When a company has a strong internal control infrastructure — including a whistleblower hotline — to combat and prevent fraud, any employee who wants to expose fraud will have a clear and confidential means of doing so. After an acquisition, employees being integrated from the acquired company will need to understand and fit into that anti-fraud culture.

This internal control infrastructure is a particularly important means of policing executive actions. Executives under pressure to boost performance during the recovery could be tempted to manipulate financial statements or perpetrate fraud in a federal contracting business. For example, the head of a government contracting business might overcharge the federal government for services not rendered or reduce project costs to the company by using inferior materials.

One famous — albeit older — example is WorldCom's troubles in 2001, when the company bought up small telecom providers. To improve financial results, management took the expenses related to these acquisitions off the books and recategorized them, while also inflating inventory and other assets to improve the balance sheet. As soon as WorldCom couldn't make its earnings targets, the company was under pressure to sell overvalued assets and do more maneuvering to avoid exposing the fraud, ultimately forcing it into a vicious cycle.

### Fraud response

More broadly, management needs an incident response and tracking mechanism to stay abreast of any issues that may arise. Through such a mechanism, any allegation or complaint anywhere in the organization can be captured in one central place. If a manager has been cited for expense report aggressiveness multiple times but has not received a warning or been subject to disciplinary action, a widespread breakdown in training, supervision and management may have taken place. Therefore, it is important for senior management to have the means to identify these types of problems before they become endemic and undermine the company's culture.

Publicly traded companies are required to have a whistleblower hotline in place. Some companies have nothing more than a toll-free hotline that goes into the voice mail of the HR director, even though few potential whistleblowers want to be identified via voice mail. A better approach is to outsource hotline management to an independent third party so that the hotline can operate 24 hours a day with anonymity preserved. Callers will receive a code to follow up for more information or to collect a reward. There should also be a way to funnel hotline claims to the appropriate area for investigation. Depending on the type of issue involved, the appropriate party to investigate a claim could be the general counsel, audit committee chairman, compliance department, HR or any combination of these. However, one designated department or individual must have ownership of all whistleblower claims to ensure that investigations are thorough and timely.

### Update fraud prevention tools constantly

Internal controls, due diligence and other fraud prevention tools are works in progress. There are constant pressures and developments that affect the incidence of fraud and make an organization more or less vulnerable to it. Effective monitoring of controls not only enables the preparation of accurate and timely financial statements, but also allows companies to provide periodic certifications or assertions regarding the effectiveness of their internal controls.



During 2009, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published *Guidance on Monitoring Internal Control Systems*, which focuses on continuous monitoring of internal controls to ensure that they consistently produce accurate and reliable information for use in decision-making. In addition, the guidance reinforces the importance of separate evaluations of internal controls, including internal audit, and appropriate oversight of governance by the board of directors.

### **Preventing fraud in government spending**

Because it is much harder to retrieve funds after they have been disbursed, effective anti-fraud activity starts with prevention. Although the federal government is leveraging technology to make sure the right payment in the correct amount is made to the right contractor, fraud prevention remains a major challenge, and some agencies and contractors are further along in these efforts than others.

Adding a layer of monitoring — such as the establishment of the Recovery Accountability and Transparency Board set forth in the ARRA — can also help. This monitoring activity can include the regular review of reports by someone independent of the spending, as well as proper and timely reconciliations that are conducted and reviewed by someone who does not create them. Conducting a risk assessment of operations can help identify the overall potential for fraud, as well as the general strengths and weaknesses of the controls. Testing can reveal whether a company's fraud protection and internal controls are robust enough or, alternatively, whether corrections are necessary.

Here are some ways to begin establishing fraud prevention efforts and programs.

### **Develop metrics and controls**

Monitoring and reporting require specific metrics and key risk indicators that, in turn, can aid the development of internal controls along the pipeline that delivers federal funds to contractors and other recipients. Because governments have struggled to achieve universal accuracy in reporting data about the disbursement of funds, this approach requires a new way of conducting business. For example, even if a government entity (federal, state or local) has effective internal controls and pays a company the right amount to build a road or bridge, the entity still needs to know how that company used those funds and whether it has appropriate internal controls of its own.

Vigilance and logic have to be built into internal controls to ensure proper stewardship of government funds. In this example, continuous auditing and value-based data analytics would bring a reasonable level of control monitoring to bear.

### **Be prepared to justify the need and the cost**

Fraud prevention comes with a cost that can be hard for a government contractor to justify, particularly if the payoff is not readily apparent. Government agencies have limited budgets and are constantly challenged to manage finite resources to meet competing demands. In many cases, this doesn't leave much room for attention to internal controls or fraud prevention. Contractors are in the same position because they are going up against competitors in situations where pricing and cost structure could be the difference between winning and not winning the business.

Just as individuals may decide to purchase security systems once they have experienced a robbery or a house fire, contractors may be more inclined to spend on fraud prevention if they have already been subject to an investigation or experienced a serious fraud incident involving government funds.

### **Prescreen for emergencies**

To deal with emergency situations where internal controls can be weakened, government agencies can prescreen contractors based on such criteria as financial stability, years in existence, or credit rating. By setting up a process for advance clearance of contractors assigned to help during an emergency or disaster, government agencies can vet contractors for appropriate internal controls and financial stewardship before the emergency occurs. The U.S. Department of Homeland Security is moving toward giving qualified vendors preclearance for disaster relief.

### **Learn from the past**

Contractors need to be responsive and make sure that they are administering programs effectively with stronger and better internal controls. They can learn from past experiences in dealing with actual fraud and in identifying potential fraud and areas of weakness. It is also essential to maintain adequate reporting and transparency and to establish and maintain effective whistleblower programs.

# Conclusion

Companies that reaffirm and reinforce their internal controls, due diligence and other fraud prevention activities are positioning themselves to take advantage of recovery-generated opportunities as well as other changes to the business environment.

With greater financial regulation on the horizon and a stronger government approach to anti-fraud activities, the fraud prevention steps outlined in this paper will become essential elements of any successful business going forward. By taking steps now to evaluate current internal control structures and due diligence processes, companies can address any weaknesses and identify potential improvements. In doing so, they are strengthening the chances that their future growth will not be diminished or derailed by fraudulent activity.

Beyond the current need for strong fraud prevention, management teams would be well-served to embrace an ongoing approach to internal control and fraud prevention that meets the needs of the company and its shareholders, employees and other key stakeholders. It is a balancing act between the cost of maintaining internal controls, the cost of implementing other fraud prevention techniques, the cost of auditing for compliance, and the benefits derived. Management teams and their boards need to make sure they understand the risks facing their organizations; furthermore, they must be confident that they have devoted the appropriate level of financial, physical and human resources to strike a balance between too much control and too little.



# About the authors



**Warren Stippich**  
Partner, Business Advisory Services  
T 312.602.8499  
E Warren.Stippich@gt.com

Warren Stippich is a partner and the practice leader of Grant Thornton LLP's Business Advisory Services group in Chicago. In addition, he is the National Governance, Risk and Compliance Solution Leader. He has more than 19 years of experience working with multinational, entrepreneurial and high-growth public companies. Stippich brings experience to the business risk consulting and internal audit services areas from both public accounting and industry perspectives.

Stippich is a CPA (Illinois), a Certified Internal Auditor and a Certified Business Manager. He is a member of the American Institute of Certified Public Accountants, the Illinois CPA Society and the Institute of Internal Auditors. Stippich received his B.S. in accountancy from the University of Illinois at Urbana-Champaign.



**Mark Sullivan**  
Principal, Economic Advisory Services  
T 312.602.8110  
E Mark.Sullivan@gt.com

Mark Sullivan is a principal and the practice leader of the Forensic and Investigative Services practice in Grant Thornton's Chicago office. Sullivan specializes in corporate investigations, fraud prevention and detection, and litigation support. For more than 25 years, he has worked with companies and their counsel worldwide to investigate instances of fraud, develop and implement anti-fraud programs, and identify vulnerabilities within their organizations. Sullivan has managed numerous high-profile investigations resulting in criminal and civil convictions related to vendor fraud and kickbacks, data breaches, and various conflicts of interest.

Sullivan is a Certified Fraud Examiner, a Certified Forensic Interviewer and a Certified Protection Professional. He earned his B.S. from Southern Illinois University in administration of justice.

## The authors would like to thank the following contributors for their valuable insights and comments:

**James G. Huse, Jr.**  
Senior Advisor, Program Integrity and Investigations, Global Public Sector  
T 703.373.8654  
E James.Huse@gt.com

**Steve Brady**  
National Managing Partner, Transaction Advisory Services  
T 312.602.8556  
E Steve.Brady@gt.com

# Resources

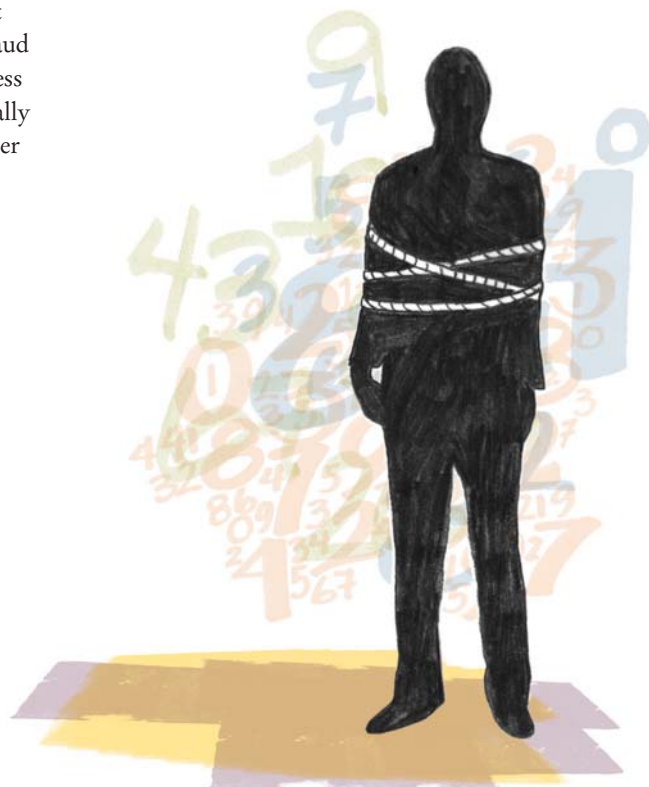
For companies considering the steps necessary to prevent fraud and mitigate fraud risks, the following resources are available to support those efforts.

*Guidance on Monitoring Internal Control Systems* has been released by the Committee of Sponsoring Organizations of the Treadway Commission (COSO); a diverse Grant Thornton team led the initiative. The purpose of the guidance is to assist organizations in monitoring the effectiveness of their internal control systems and taking timely corrective action as needed.

*The Audit Committee Handbook, Fifth Edition*, by Grant Thornton's R. Trent Gazzaway, national managing partner of audit services, and Robert H. Colson, partner in public policy and external affairs, has expanded its coverage of managing fraud risk. Although audits historically have not included risk assessment and management, today's audit committees increasingly have a responsibility to consider fraud risk and to ensure that companies are doing enough to address that risk. This is particularly true as companies expand globally and find themselves exposed to new fraud risks that had never been an issue before.

*The Anti-Corruption Handbook: How to Protect Your Business in the Global Marketplace* by Grant Thornton's William P. Olsen is designed to help senior managers and executives responsible for fraud detection meet the challenges of maintaining business integrity in the global marketplace and mitigating emerging risks. The book provides insight into:

- the internal controls and accounting provisions of the FCPA and other U.S. laws governing corruption, anti-money laundering, procurement and construction fraud;
- information security; and
- the design and administration of effective whistleblower programs.



# Grant Thornton offices

## National Office

175 West Jackson Boulevard  
Chicago, IL 60604  
312.856.0200

## National Tax Office

1900 M Street, NW, Suite 300  
Washington, DC 20036  
202.296.7800

## Arizona

Phoenix 602.474.3400

## California

Irvine 949.553.1600  
Los Angeles 213.627.1717  
Sacramento 916.449.3991  
San Diego 858.704.8000  
San Francisco 415.986.3900  
San Jose 408.275.9000  
Woodland Hills 818.936.5100

## Colorado

Denver 303.813.4000

## Florida

Fort Lauderdale 954.768.9900  
Miami 305.341.8040  
Orlando 407.481.5100  
Tampa 813.229.7201

## Georgia

Atlanta 404.330.2000

## Hawaii

Honolulu 808.536.0066

## Illinois

Chicago 312.856.0200  
Oakbrook Terrace 630.873.2500

## Kansas

Wichita 316.265.3231

## Maryland

Baltimore 410.685.4000

## Massachusetts

Boston 617.723.7900

## Michigan

Detroit 248.262.1950

## Minnesota

Minneapolis 612.332.0001

## Missouri

Kansas City 816.412.2400  
St. Louis 314.735.2200

## Nevada

Reno 775.786.1520

## New Jersey

Edison 732.516.5500

## New Mexico

Albuquerque 505.855.7900

## New York

Long Island 631.249.6001  
Downtown 212.422.1000  
Midtown 212.599.0100

## North Carolina

Charlotte 704.632.3500  
Greensboro 336.271.3900  
Raleigh 919.881.2700

## Ohio

Cincinnati 513.762.5000  
Cleveland 216.771.1400

## Oklahoma

Oklahoma City 405.218.2800  
Tulsa 918.877.0800

## Oregon

Portland 503.222.3562

## Pennsylvania

Philadelphia 215.561.4200

## South Carolina

Columbia 803.231.3100

## Texas

Austin 512.391.6821  
Dallas 214.561.2300  
Houston 832.476.3600  
San Antonio 210.881.1800

## Utah

Salt Lake City 801.415.1000

## Virginia

Alexandria 703.837.4400  
McLean 703.847.7500

## Washington

Seattle 206.623.1121

## Washington, D.C.

Washington, D.C. 202.296.7800

## Wisconsin

Appleton 920.968.6700  
Madison 608.257.6761  
Milwaukee 414.289.8200



© Grant Thornton LLP  
All rights reserved  
U.S. member firm of Grant Thornton International Ltd

#### About Grant Thornton's Advisory Services Practice

Today you need advisors that focus on insightful and innovative solutions for your complex issues, such as complying with changing legislation, managing risk, containing costs, streamlining business processes and identifying strategic transaction opportunities. Grant Thornton's Advisory Services professionals can deliver value by providing independent advice to public, private and not-for-profit organizations. Our specialists combine insight and innovation from multiple disciplines with a wide range of business and industry knowledge. To learn more, visit [www.GrantThornton.com/advisory](http://www.GrantThornton.com/advisory).