Advisory
Forensic Services

Cracking down*

The facts about risks in the procurement cycle

*connectedthinking

PricewaterhouseCoopers

Table of contents

The heart of the matter

The risk of waste, abuse, and fraud in procurement is real and pervasive

Preventing waste, abuse, and fraud in procurement (procurement risk) is a considerable challenge. Given the increasing focus of law enforcement on corporations in recent years, it is critical to understand the trends in procurement operations and in enforcement. To avoid and limit the legal and financial risks of procurement fraud, it is equally important to recognize the enforcement strategies of state and federal government agencies that interface with contractors and service providers.

The $787 billion federal stimulus package includes as much as $100 billion for technology initiatives and infrastructure spending, which comes with a commitment to avoid the fraud and abuses that surfaced in the aftermath of Hurricane Katrina and during the wars in Iraq and Afghanistan. It appears certain there will be limited tolerance for corporate lapses of integrity in the procurement process at the federal, state, and local government levels.

How can corporations and contractors comply with procurement guidelines and implement effective control systems to combat procurement fraud? Addressing these challenges requires an understanding of how procurement fraud is perpetrated, how it is prosecuted, and how procurement risk can be affected by corporate compliance and prevention programs.

Obtaining a good understanding of procurement risk is challenging—the facts are elusive. Comparative information about procurement fraud cases within corporations is rarely gathered and published; therefore, public, authoritative data is scarcely available. Instead, managers, boards, and legislators are forced to rely on perceptions rather than facts when making decisions regarding budgets and resources. The following views toward procurement risk are, in fact, misperceptions:

- Procurement risk and corruption are limited to the developing world.
- Procurement risk in the United States mainly affects defense contractors.
- Procurement risk is a peripheral issue for corporations with codes of ethics and ethics hotlines.
- Compliance with the internal controls provisions of the Sarbanes-Oxley Act eliminates procurement risk.

The enforcement actions of the National Procurement Fraud Task Force (Task Force) have improved understanding of procurement risk. The Task Force represents a coordinated effort by the Department of Justice (DOJ) and other agencies to focus on the detection, prevention, and prosecution of procurement fraud.[1]

Task Force data—including schemes, industries, and perpetrators—can inform private-sector corporations engaged in significant contracting activities and provide a useful road map regarding the complexities and risks associated with procurement. Analysis of the enforcement activity demonstrates that procurement risk extends across a multitude of industries, and schemes vary in nature, complexity, and scale. With increased calls for accountability from corporations providing goods and services to all levels of government, those that fail to establish effective controls may face significant legal and brand damage.

[1] PricewaterhouseCoopers (PwC) recognizes the limitations associated with data and information published by the Task Force. PwC is aware that this data is not all-inclusive. The DOJ uses a variety of sources to populate its website and attributes to the Task Force all prosecutions and convictions reported to it by the US attorneys offices, whether there is a Task Force nexus or not.

An in-depth discussion

Data shows procurement risk stems from vulnerabilities in corporate controls

On March 4, 2009, President Barack Obama ordered an overhaul of the federal contracting system, stating, “We’ll have to break bad habits that have built up over many years.”[2]

Presidential attention to issues of procurement is not an ordinary matter and may mark a sea change in public expectations, lawmakers’ actions, and corporate responses to this emerging risk.

Federal efforts to combat procurement fraud are not new. The National Procurement Fraud Task Force was created in October 2006 to help shed light on procurement fraud schemes through the prosecution of perpetrators. Its actions have reinforced that procurement fraud is often perpetrated by individuals with significant operational knowledge of the systems they abuse, and the crime is becoming progressively more elaborate and technology-driven.

PricewaterhouseCoopers’ (PwC) review of the Task Force’s enforcement data serves as a valuable tool to understand common themes in procurement fraud. Spearheaded by the DOJ, the Task Force brings together representatives from the DOJ, the FBI, federal inspectors general, defense investigative agencies, and federal prosecutors from US attorneys offices across the country. Its goals are to fight procurement fraud’s myriad schemes by increasing civil and criminal enforcement, as well as to “focus on maximizing information sharing and take significant leadership in addressing issues such as grant fraud, relations with the private sector, training, and legislation.”[3]

Analysis of the Task Force’s activity[4] illuminates some of the trends and business dynamics behind the government’s flurry of prosecutorial activity. Since the creation of the Task Force, more than 400 procurement fraud cases have been pursued. These cases have resulted in more than 300 criminal convictions and the recovery of hundreds of millions of dollars in civil settlements and judgments.[5] As of November 2008, the DOJ had filed numerous criminal charges related to procurement fraud, particularly relating to the global war on terror.

To better understand the activity and focus of the Task Force, as well as the potential implications for contractors and subcontractors, PwC reviewed a subset of the press releases from June 2007 through June 2008. During this period, the Task Force issued press releases that related to more than 300 civil and criminal defendants.

[2] See Federal Register, Vol. 74, No. 43, p. 9755-9757.

[3] National Procurement Fraud Task Force mission statement, http://www.usdoj.gov/criminal/npftf/.

[4] Task Force press releases are available at http://www.usdoj.gov/criminal/npftf/pr/press_releases/.

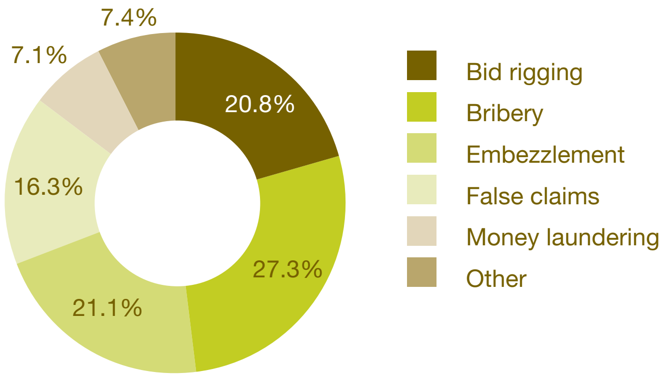
[5] National Procurement Fraud Task Force Progress Report, December 2008.

Common procurement fraud schemes

Waste, abuse, and fraud in procurement are manifested in a variety of schemes including bribery, bid rigging, embezzlement, money laundering, and false claims, as detailed in Figure 1.

The types of fraud schemes continue to evolve. In fact, during the 13-month period of Task Force activity reviewed, more than 500 schemes or combinations of schemes were investigated. The vast majority of prosecutions pursued by the Task Force address bribery, bid rigging, embezzlement, and false claims.

Figure 1: Types of fraud schemes investigated by Task Force (June 2007–June 2008)



Bribery and bid rigging

Anti-competitive behavior can take several forms. It includes defendants engaged in influencing the outcome of tendering processes, offering and accepting bribes, and colluding with others to fix prices and influence contract allocations (commonly referred to as bid rigging). Variations of bribery and bid rigging accounted for almost 50 percent of the schemes identified by the Task Force.

Bribery was the most prevalent type of scheme prosecuted by the Task Force, accounting for 158 (27.3 percent) of the schemes identified. Cases involving bribery represent some of the most objectionable abuses of authority and often involve experienced employees. Common examples include public servants accepting bribes to steer contract awards or employees accepting kickbacks from vendors in return for allowing overcharging. The latter occurred in January 2008 when officials from the North Carolina Department of Transportation demanded a 10 percent kickback on any contracts awarded for maintenance projects.

Bid-rigging schemes often involve bribery. However, anti-competitive behavior that does not involve bribery exists when groups of contractors collude to rig bids, fix prices, and allocate market share to inflate profits across a group.

Embezzlement

Embezzlement cases often involve defendants who create fictitious companies or make submissions for payments based on fake invoices.

In one embezzlement case prosecuted by the Task Force, a distribution company collected more than $20 million in fraudulent shipping costs to supply small hardware components, plumbing fixtures, electronic equipment, and various other items to Iraq and Afghanistan. The defendants took advantage of automatic invoice processing by the Department of Defense to streamline the resupply of items to combat troops in the Middle East. The shipping costs often ran into hundreds or thousands of dollars, even though the supplies themselves rarely exceeded $100.

If convicted, the charges—conspiracy to commit wire fraud and conspiracy to commit money laundering—carry maximum penalties of up to 20 years in prison and fines of $500,000, or twice the value of the property involved.

In another embezzlement case, the owner and a vice president of a company that supplies asphalt to the Commonwealth of Massachusetts were sentenced to prison terms of 42 months and 30 months, respectively, for submitting inflated weigh bridge tickets to the government for payment. The pair were fined $150,000 and $10,000, respectively, and compelled to pay more than $300,000 in criminal restitution. The company also was fined $3 million and given four years of probation.

False claims

Another significant category of defendants includes those charged with breaching the False Claims Act (FCA). The federal FCA prohibits individuals or companies from making demands for payment or withholding funds that they are not entitled to receive. The Act applies to entities that do business with the federal government or those doing business with corporations that are contractors of the federal government. In addition to the federal FCA, several states have enacted state FCAs, which apply to individuals and contractors that defraud state and local governments.

False claims offenses often involve making false statements about products supplied to government agencies or misleading the government as to the nature of a product or production processes used.[6]

[6] These and other procurement risk complexities associated with the aerospace and defense industry are subject to a detailed examination in the PricewaterhouseCoopers publication titled *Predicting the Unpredictable—Protecting Aerospace and Defence companies against fraud, reputation and misconduct risk* (September 2006).

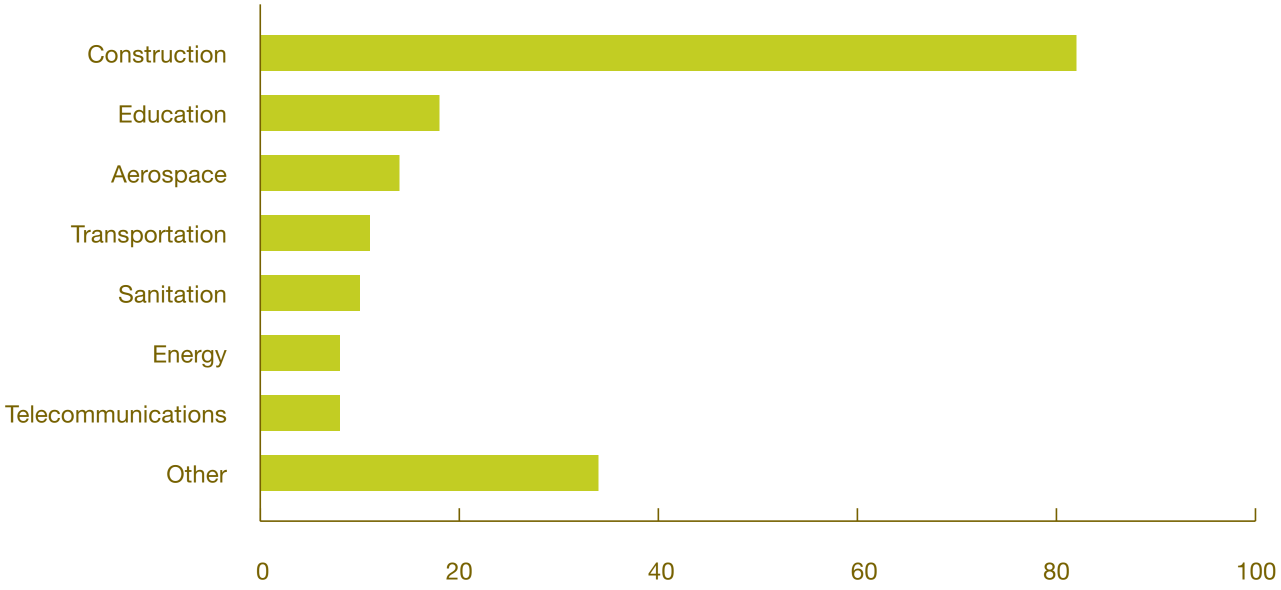
Procurement risk affects a wide range of non-military industries

PwC's experience and analysis of the Task Force data illustrate procurement risk's pervasiveness across a wide range of industries. While the government is exposed and more focused on prosecution in defense and related industries, almost two-thirds of reported cases do not involve military-related spending.

Of the non-military industries, procurement fraud cases involving the construction industry were most prevalent. Other industries that were subject to Task Force prosecutions include education, aerospace, and telecommunications. In total, from June 2007 through June 2008, procurement fraud cases involved more than 25 distinct industries.

The broad base of underlying industries supports the premise that no branch of government is immune from the risk of procurement fraud. The Army, Navy, Air Force, and Department of Defense accounted for 38 percent of prosecuting agencies, but the majority (62 percent) of cases were scattered across 62 different government agencies, from the Department of Transportation to the US Postal Service. The most prevalent non-military agencies involved in procurement fraud cases were those that most engage in contracting activity, such as the Department of Transportation, the Department of Housing and Urban Development, and the Department of Education.

Figure 2: Task Force cases involving non-military industries

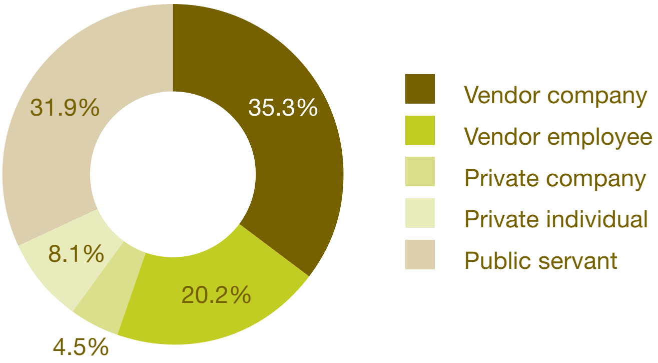


Offenders come from all types of backgrounds

Describing a “typical” procurement fraud perpetrator can be difficult. Both corporations and individuals are prosecuted, and individuals’ roles vary widely. The Task Force has prosecuted a range of individuals, from senior ranking officers in the US Army who had received bribes close to $10 million to an employee in the graphics center of an educational institution who embezzled $1.2 million through payment of fake invoices.

Figure 4 identifies the types of defendants subject to Task Force prosecution from June 2007 through June 2008.

Figure 4: Types of defendants prosecuted by Task Force



More than half of defendants were vendors or their employees, and a significant proportion of cases—close to 32 percent—involved public servants. This finding underscores how purchasing authority tempts individuals engaged in procurement activities in the public or private sectors. Employees who abuse their authority, show favoritism, or condone or permit conflicts of interest demonstrate poor business judgment, and these actions may be early indicators of potential collusive behavior.

This is exactly why processes need to be strong and the effectiveness of controls should be periodically monitored and evaluated. The true test of whether a corporation's internal controls environment is effective and its ethics and compliance program is robust is when it faces possible collusion between vendors and employees or learns of demands for kickbacks.

The variety of industries, plethora of government agencies involved, and the spread of the crime's geographical reach indicate that the common denominator of procurement fraud is vulnerability in corporate controls.

Government contractors face increasing legal and financial risks

The ultimate risk of prosecution, suspension, and debarment has been historically borne by large federal contractors. However, recent changes to federal regulations, the expected growth in federal, state, and local contracting activity, and vigorous enforcement activity increase procurement risk for smaller corporations, especially those that do not traditionally focus on selling goods and services to the public sector. These trends should be carefully evaluated by contractors. Particular care should be taken by smaller corporations and subcontractors, especially those whose compliance and antifraud procedures have not yet been subject to detailed independent testing.

Changes to Federal Acquisition Regulation (FAR) pose additional challenges

Corporations that contract with the federal government are required to be fully compliant with FAR. Recent revisions to FAR intensify the inherent challenges of complying and reporting potential abuses, and the impact of changes to disclosure rules will be substantial, particularly for midsize companies.

On November 12, 2008, the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council published a rule on contractor business ethics compliance programs and disclosure requirements.[7] This rule, effective December 12, 2008, expands the scope of the existing FAR business ethics and conduct clause[8] to include causes for suspension or debarment. These causes now include federal contractors who:

1. Knowingly fail to timely disclose certain criminal offenses and violations of the civil False Claims Act (FCA)

2. Knowingly fail to timely disclose credible evidence of significant overpayments (other than overpayments resulting from contract financing) related to the award or performance of a contract or subcontract.[9]

[7] FAR Case 2007-006, Contractor Business Ethics Compliance Program and Disclosure Requirements, Federal Register, Vol. 73, p. 67064.

[8] FAR 52.203-13, Contractor Code of Business Ethics and Conduct.

[9] Further discussion of changes to FAR is available in technical alerts produced by PwC's Government Contracts practice, including an Ethics and Compliance alert.

An earlier amendment to FAR[10] mandates reporting requirements for companies with federal contracts of $5 million or more that have performance periods of 120 days or more. The rule states that these contractors must have a written code of business ethics and conduct and an ethics compliance training program for their employees.[11]

To further strengthen compliance, the Task Force has asked the FAR Council to publish a rule that would require service contractors to provide annual certifications regarding their employees.[12] The new and proposed rules clearly amend the status quo that existed between contractors and the federal government regarding the disclosure of certain criminal and ethical violations. The most recent rule passed after considerable opposition by the contractor community, and several key terms, such as "significant overpayments," remain open for interpretation.

According to Eric Feldman, co-chairman of the Private Sector Outreach Committee of the Task Force and the senior advisor to the director of the National Reconnaissance Office for Procurement Integrity, the effects of the amended FAR disclosure rules will be substantial.

"The new FAR mandatory disclosure rule may greatly impact those midsize companies that do not have a mature business ethics and compliance program but now fall within the $5 million threshold," said Feldman. "I would also assert that some of the larger companies that were required under Sarbanes-Oxley to create such a program may have done so in a manner that places form over substance and the spirit in which these programs were originally intended. I believe that some of the larger programs may be 'paper tigers' that operate without the benefit of adequate numbers of trained, experienced personnel conducting internal investigations and training the workforce."

[10] Effective December 24, 2007.

[11] Federal Register, Vol. 72, p. 65873.

[12] The annual certification is designed to ensure that entities have: 1) trained their employees on the relevant responsibilities and restrictions to which they are subject while performing government work; and 2) collected from their employees the financial information necessary to identify and to screen out employees with personal conflicts of interest. The Task Force recommended that both training and the financial conflicts review be completed before a contractor assigns employees to perform work for the government under a service contract. Recently, the FAR Council announced its intention to publish in 2009 a proposed FAR rule that addresses conflicts on the part of service contractor employees.

In light of the complexities associated with determining what constitutes a "significant" overpayment or fraud, companies should develop a detailed process that includes a careful analysis of facts and circumstances. Further, qualified counsel and forensic specialists should be engaged before making any reporting decisions regarding matters that may potentially stem from fraudulent activity.

Feldman echoed these concerns: "Under the new FAR requirements, it is expected that companies will do their own internal investigations to determine whether there is 'credible evidence' to be reported to the government. In my experience, companies have used HR officers, lawyers, security people, and other unqualified non-investigators to do this kind of work."

State and local governments step up enforcement efforts

The federal government is not the only one responding to procurement fraud. The Deficit Reduction Act of 2005, enacted on February 8, 2006, contained provisions that create incentives for states to enact antifraud legislation modeled after the FCA. Many states have had civil false claims acts focusing on Medicaid fraud, but few have modeled their statutes on the federal FCA.

Recently, however, more than 20 states and cities including New York and Chicago have followed the federal government's lead by enacting their own civil false claims acts. The incentive for states to enact such legislation is to get a higher percentage of amounts recovered in false claims actions brought under state regulations.

Another significant development is the passing of a whistleblower rights law as part of the $787 billion stimulus spending bill. The final stimulus package includes “best practices” anti-retaliation rights for any workers at recipients of the new federal spending. This includes contractors, grantees, and state and local government employees who work in programs that receive stimulus funding.

State and local governments are also taking action against vendors and service providers who perpetrate procurement fraud. Recent reported cases include:

- On October 7, 2008, the Chicago Department of Procurement Services and the Chicago Office of the Inspector General announced the proposed debarment of 23 businesses and 26 affiliated individuals in connection with allegations of various fraud-related activities[13] including forgery, bribery, mail fraud, and witness tampering.
- According to an Inspector General’s report issued October 16, 2008, three employees of Ohio Department of Transportation (ODOT) accepted about $390,000 in gratuities and improper payments from nearly three dozen ODOT vendors in exchange for steering business to them by altering bid documents and sharing bid information with favored vendors.[14]
- On December 22, 2008, the Port of Seattle’s executive director issued a plan featuring disciplinary actions and new compliance policies in response to a recent port probe that found multiple instances of fraud committed by port employees. Fraudulent activities included steering contracts to favored vendors and multiple bid-rigging schemes.[15]
- On January 6, 2009, New York State Comptroller Thomas P. DiNapoli announced that his auditors identified more than $1 million in purchases that involved improper collusion with vendors and bid rigging at the Central New York Developmental Disabilities Services Office. Auditors found that physical plant staff colluded with at least nine favored vendors, some of whom were family and friends of staff, who would submit fake bids for sham entities—and even legitimate companies—to receive state business.[16]

[13] City of Chicago, http://egov.cityofchicago.org/city/webportal/jsp/content.

[14] Ohio Department of Transportation, “Report on Investigation,” http://www.watchdog.ohio.gov/investigations/2007100.pdf.

[15] http://www.shippingdigest.com/news/article.asp?sid=5744&ltype=maritime.

[16] http://www.wktv.com/news/local/37142489.html.

Procurement risk in the private sector—an increasing challenge

Procurement risk schemes involving collusive bidding, bid rigging, bribes, and embezzlement against corporations in the private sector are similar to those in the public sector. This is not surprising. The key factor leading to procurement risk is the same: a control environment that allows misconduct or fails to prevent or timely detect procurement schemes.

A key differentiator between the private and public sectors is that corporations have an inherent incentive to achieve profitability and are focused on receiving the best price or highest quality product or service from their vendors. Irregularities in the procurement process should, theoretically, be prevented and detected more effectively.

Investigations of procurement risk in corporations typically are conducted internally to protect the corporation's business interests and employee confidentiality. Occasionally, the actions of employees and vendors involved in procurement schemes are made public through criminal prosecution or civil procedures, but often these acts simply result in the severing of employment or business relationships. Corporations' preference to keep matters behind closed doors is understandable, but it also skews perceptions about the pervasiveness of procurement risk.

Operational gaps increase procurement risk

Because procurement fraud and abuse often are perpetrated by individuals with significant operational knowledge of the systems and processes they abuse, offenders tend to operate "under the radar." The challenges that organizations face in complying with and enforcing policies related to bidding processes, information management, vendor maintenance, and invoice and payment processing create opportunities for abuse and make it difficult to detect and prevent fraud and corruption. Conversely, addressing known and suspected instances of waste, abuse, and fraud in procurement closes operational gaps and generates opportunities to introduce transparency, develop integrity, and realize cost savings.

To help identify operational gaps that expose organizations to greater risk of waste, fraud, and abuse in the procurement cycle, it is beneficial to look closely at process inefficiencies, unnecessarily high administrative costs, shrinkage, and spend leakage. Each of these factors could indicate poorly designed procurement processes. When multiple red flags are evident, procurement risk increases and should be more carefully evaluated. Examples of potential red flags for procurement risk include:

Information management

- Inconsistent data across procurement-related systems
- Data quality issues relating to spend data and vendor data
- Lack of transparency of procurement data
- No structured approach to consolidate, cleanse, and enhance procurement data

Procurement process

- Lack of controls around use of preferred vendors, negotiated contracts
- Low compliance with corporate preferred buying guidelines
- Buying power not fully leveraged due to lack of reporting/knowledge of historical spend

Vendor maintenance

- Multiple instances of the same vendor within master file
- Inconsistent vendor payment terms across the organization
- Lack of controls around vendor creation and management
- Failure to actively manage high-risk vendor relationships

Invoice and payment processing

- Duplicate payments
- Inefficient invoice processing
- Failure to optimize cash flow and payment terms to vendors and suppliers
- Limited segregation of duties involving payments, credits, and reconciliation of vendors/suppliers

Identifying and acting against a successful perpetrator

The challenge

A successful plant manager in the Texas subsidiary of a European-based corporation had a reputation of disregarding directives imposed by the parent company. In addition, he had a propensity to retain vendors that were not on the corporation's preferred vendor list, and personal relationships with senior personnel at various vendors were considered improper by staff and peers. An employee dismissed by the plant manager sent an anonymous complaint to corporate headquarters and two major clients. An investigation by an independent third party revealed personal relationships with vendors had been concealed and kickbacks had been paid to a straw company.

What the organization could do better

The plant manager's success in running the local facility caused many of his supervisors to turn a "blind eye" to lapses of business judgment. Strict enforcement by the corporation of procurement guidelines—including purchasing from preferred vendors—may have prevented the illicit contracting. In addition, detailed due diligence procedures regarding new vendors would have revealed that a vendor company did not have significant business history. A better process of monitoring employee concerns regarding ethics may have accelerated the discovery of fraudulent activity.

Key takeaways

Procurement fraud often is perpetrated by individuals who have detailed knowledge of bidding, ordering, shipping, billing, and payment systems, or those who have the authority to override these systems. The challenge faced by many corporations is to prevent tampering in the first place. In cases of abuse or fraud in the procurement cycle, it is crucial for corporations to demonstrate zero tolerance. Striking the right balance between "micro-management" and tolerating potential misconduct is difficult and requires a careful consideration of competing factors.

Sarbanes-Oxley compliance does not guarantee elimination of procurement risk

A common misconception of corporate executives is that the significant time and resources poured into strengthening internal controls to meet Sarbanes-Oxley's requirements are a cure-all in the fight against fraud, in general, and procurement risk, in particular. In fact, the Sarbanes-Oxley Act relates to internal controls over financial reporting and fraud management processes, but these controls may be less effective against procurement risk schemes.

One reason Sarbanes-Oxley compliance does not eliminate procurement risk is due to the typical profile of perpetrators. Because they often possess intimate knowledge of internal systems, fraudsters who successfully perpetrate their fraud schemes over long periods usually do so by operating under monetary thresholds determined for Sarbanes-Oxley testing purposes.

Further, as industries consolidate under the pressure of globalization, corporations' purchasing operations grow increasingly larger in size and complexity. This growth leaves them more vulnerable to the risk of abuse in the procurement cycle. Despite the internal control requirements of Sarbanes-Oxley, corporations should avoid complacency in their compliance efforts.

Though fraud and abuse in a corporation's procurement cycle represent formidable challenges, a notable silver lining may exist in the opportunities to realize significant cost savings. Incidents of fraud and risk factors of possible fraudulent activity shed light on where to tighten operational controls and where to shave costs. Corporations also may leverage their better understanding of spend to consolidate vendors and streamline their procurement processes. Further, strengthened IT systems may significantly benefit a corporation by focusing on the establishment and maintenance of vendor master files and other support systems that traditionally are more vulnerable to abuse.

Sorting out waste from fraud

The challenge

A multinational financial institution faced concerns of waste and inappropriate use of funds allocated to projects executed in locations distant from its headquarters. Additionally, management needed to determine whether it was dealing with inefficiencies and waste by its senior local staff or with intentional misconduct. Before reaching a conclusion, the institution had to analyze business practices around the project life cycle and assess risk factors in the procurement of goods and services. Detailed analysis of purchase orders and contract data was needed to help determine what information is collected and used prior to making purchasing decisions and whether local management was aware of known instances of vendor underperformance.

What the organization could do better

The institution should have had a robust process of evaluating fraud risk at its regional business unit. The assessment should have focused on soundness of procurement policies, procedures, and practices in the areas of antifraud, anticorruption, governance, and key fiduciary matters. A periodic evaluation of the procurement function's structure and its performance was warranted. This evaluation would have disclosed a culture of disregard by junior professional staff for corporate requirements of segregation of duties. Monitoring compliance with headquarters' procurement guidelines and the effectiveness of related internal controls would have revealed that site visits were not conducted or their results were ignored.

Key takeaways

When dealing with procurement risk, it is crucial to recognize that gaps in controls contribute to inefficiencies in operations, and they often may be harbingers for intentional abuse. By tolerating disregard of operational and ethical controls, allowing blatant inefficiencies in project execution, or consenting to vendor noncompliance, managers can more easily conceal that they are personally benefiting from the situation.

Instances of procurement fraud are more frequent than commonly realized

Limited focus on the ever-growing volume of transactions and the monetary value processed by already strained procurement systems and personnel—as well as the false sense of comfort that post-Sarbanes-Oxley internal controls are sufficient to prevent and detect procurement fraud—often results in a surprising number of procurement risk issues.

It is difficult to quantify the frequency of and monetary losses associated with procurement fraud in the private sector because statistics are scarce and vary significantly. Additionally, the proliferation of electronic signatures, emails, and online approvals of purchase orders, invoices, and payment requests makes it extremely taxing to prove specific individuals were working outside their authority when the unauthorized actions were taken.[17]

PwC's growing body of experience indicates that corporations and other organizations have greater exposure to procurement fraud than most senior managers and board members realize.

This point of view is shared by some of the largest insurance carriers, which often bear the economic price for procurement fraud schemes. According to Chubb Group of Insurance Companies: "Mergers, acquisitions, downsizing, restructuring, rapid expansion, and globalization have increased the challenges of maintaining a strong system of internal controls. Likewise, the expansion of computers has drastically changed the speed with which fraud can occur."[18]

Worldwide Crime Product Manager Greg Bangs at Chubb states that procurement fraud is the largest crime risk exposure facing companies today and represents approximately 40 percent of the claims submitted to crime insurance carriers.

"It is our experience that procurement fraud is most frequently committed by employees acting in collusion with vendors," said Bangs. "Although it is difficult to eliminate procurement fraud entirely, the implementation of appropriate internal control procedures, including strict segregation of duties (the golden rule of internal control), can help minimize the frequency and severity of such losses."

[17] Dalit Stern, "Procurement Fraud Looms Larger with Growth of Tech, Outsourcing," *National Underwriter* (February 25, 2008).
[18] http://www.chubb.com/businesses/csi/chubb850.pdf.

Lastly, perceptions about the frequency and severity of fraud and corruption in the US may also be impacted by the relative level of sophistication by the perpetrators. Corruption is widely believed to be an issue endemic to developing countries. However, our data reflects that bid rigging, collusive bidding, and payment of kickbacks are also prevalent in the US. The methods used by perpetrators in the US are often less direct and more difficult to detect and investigate. It is our experience that cash payments or direct wire transfers to employees' bank accounts are more common outside the US. Locally, kickbacks associated with fraud and corruption are aided by a myriad of methods including: inflated price paid in the course of purchase of assets by a vendor or associated party from a corrupt employee (real estate, art, etc.); extension of loans with unlimited terms; house improvements performed in the employee's house;
and granting of financial interest in entities.

The impact on procurement risk during economic downturns

It is important to recognize that risk increases as economic pressure mounts. The recent economic downturn leaves many corporations with limited choices regarding the need to downsize their workforce. Often, these decisions focus on functions and individuals in back-office operations. Compliance, internal audit, and finance departments are being hit harder than revenue-producing units, leaving fewer resources with greater demands on their time, and upgrades to software and hardware computer systems often are delayed.

These cost-reduction measures can impose additional resource constraints and compromise oversight and control integrity when important supervisory or monitoring functions are removed or weakened. At the same time, individuals facing serious economic distress and potential loss of income may be more likely to view the rewards of an illegitimate or fraudulent act as greater than the risk of being caught and their desire to act ethically. Vendors and service providers will feel increased pressure to get business, and some will do so using any means necessary. Familiarity of vendors and employees may become a source of increased risk. Corporations should have effective mechanisms to monitor and actively manage these potential conflicts of interest.

The causal relationship between workforce reductions and fraud is evident.

“A major reason for the increase in types of claims is cutbacks,” said Bangs. In the current economic climate, companies are reducing their workforces, often leaving disgruntled employees behind after eliminating the jobs of staff members responsible for watching out for fraud. Additionally, Bangs said, when staff is cut, those left behind often perform transactions from start to finish, largely unchecked.

Unless properly managed, cost-reduction efforts surely will undermine the progress that resulted from the Sarbanes-Oxley Act’s significant focus on internal controls.

Effective prevention and detection of procurement risk require enhancement of existing strategies and tactics

Antifraud and ethics programs have been universally revamped post-Enron, but how effective are these types of programs?

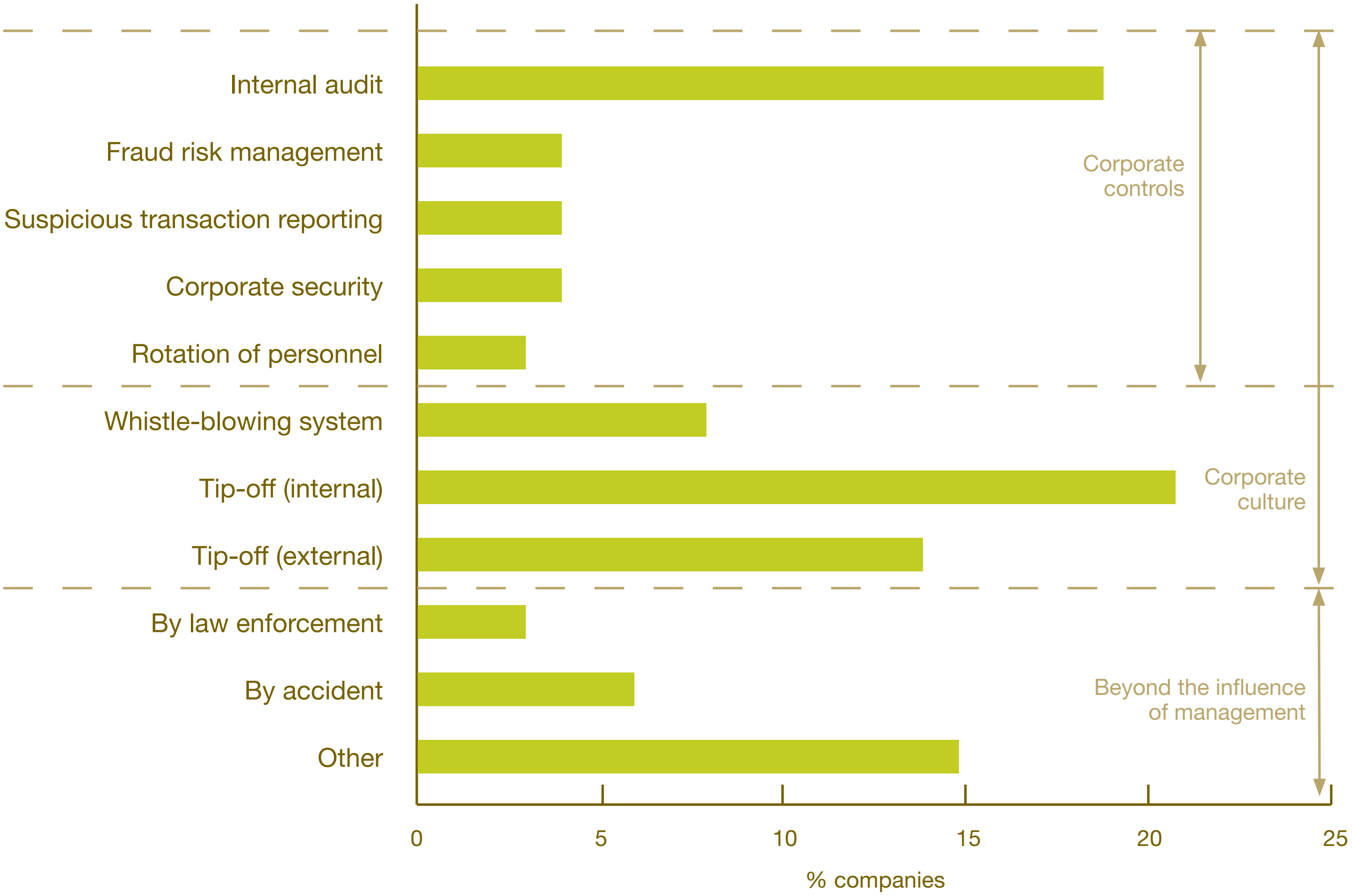
PwC research[19] indicates that controls designed to detect and prevent fraud have not proven to be uniformly effective. For example, in identifying fraud schemes, internal audit efforts accounted for only 19 percent of instances of fraud detection. In comparison, whistle-blowing systems and tip-offs accounted for 8 percent and 35 percent, respectively (see Figure 5).

Another interesting finding is that, despite considerable effort and investment in antifraud programs and fraud management, fraud was detected by these means only 4 percent of the time, which is lower than detection of fraud occurring by accident (6 percent).

“My experience is that many corporations could benefit from a combination of a self-assessment tool and a mechanism for independently assessing the viability of the programs,” said Feldman. “In addition to benchmarking best practices across industry, any assessment should examine areas such as employee training, hotline effectiveness and employee awareness, anonymous reporting processes and data security, ethical culture, and investigations.”

Feldman added that, when it comes to investigations, it is crucial to examine the qualifications of the investigators and the professionalism of the process they use.

Figure 5: Fraud detection methods in corporations



Source: PricewaterhouseCoopers, *Economic crime: people, culture, and controls—The 4th biennial Global Economic Crime Survey* (2007)

When a legitimate vendor is involved in a procurement scheme

The challenge

A publicly traded technology company suspected it had been defrauded by employees and service providers who worked closely together during a four-year period. A sophisticated series of procurement schemes required monthly and often weekly communications among the perpetrators. An investigation revealed a complex network of orders, approvals, and invoices that were based on collusion and abuse of authority and included overpayments to legitimate vendors, disbursements to fake vendors, and kickbacks paid to employees in connection with the unauthorized procurement of outsourced services. Mid-level managers in charge of outsourcing architectural and design services colluded with legitimate vendors who provided services at inflated prices that were unnecessary and inconsistent with business needs.

What the organization could do better

The illicit services were procured, approved, and paid for by employees in a manner inconsistent with the company's segregation of duties policy. In addition, leading industry practices in the areas of vendor set-up and maintenance were not followed, and payment authorization practices, use of checks, wire transfers, and interdepartmental billings were not subject to audits by the finance or budget departments. To correct these inconsistencies in the procurement system, a more transparent system of controls needs to be designed, implemented, and enforced.

Key takeaways

Unlike the use of ghost vendors, one of the most challenging aspects of procurement fraud is the use of legitimate vendors in fraud schemes. Detecting and investigating the differences between services and goods procured from a legitimate vendor for inflated prices, purchases involving incorrect quantities, and acquisitions of goods and services that were not for the organization's business purposes are difficult. Collusion between vendors and employees make these tasks even more daunting.

Corporate culture and environment are key deterrents for fraud and misconduct

Naturally, a corporation's culture and workforce environment play key roles in determining the effectiveness of fraud risk management programs.

PwC[20] research suggests that, despite significant efforts made by corporations subsequent to the Sarbanes-Oxley Act, many corporations' greatest deterrents to fraud, in general, and procurement risk, in particular, are codes of ethics and whistleblower hotlines. These are powerful tools when used appropriately and in combination with other antifraud measures. By themselves, however, they cannot be effectively relied on to prevent and detect instances of procurement fraud. PwC research also indicates that companies with both robust ethical guidelines and compliance programs report suffering fewer economic crimes than those who do not.[21]

"Data from the Ethics Resource Center and Ethicstat suggests that, in many large companies, there is a lack of confidence among the workforce in the company's commitment to business ethics and the ability of the company to keep complaints anonymous and take action in response to employee concerns," said Feldman. "Midsize companies that are just putting together a business ethics and compliance program could greatly benefit from some of the lessons learned—missteps—of some larger companies."

Where procurement fraud flourishes

PwC experience indicates that, regardless of industry, fraud, in general, and procurement fraud, in particular, are more likely to occur in the following circumstances:

- When companies exit certain operations (they anticipate taking a considerable hit to their profit-and-loss statements so oversight may be weak in these soon-to-be-discontinued activities)
- Where morale is low and staff turnover is high (especially in units where employees are being terminated and the outlook for a unit's survival is bleak)
- In sectors, units, and geographies that previously enjoyed rapid growth and outgrew their controls
- In units that are geographically remote from corporate headquarters
- In operations, processes, and activities that are not central to an organization's core business (e.g., printing, food services, construction)

[20] PricewaterhouseCoopers, *Economic crime: people, culture, and controls—The 4th biennial Global Economic Crime Survey* (2007).

[21] Ibid.

The hiring process only adds to the procurement risk most companies face.

"Companies generally recognize that background checks of employees are an important loss-prevention tool, but they may not actually check employee references or perform background checks in practice," said Bangs.

PwC experience suggests that procurement risk increases when corporations execute no or only limited levels of initial due diligence on their vendors. Further, periodic due diligence of vendors should be performed using a risk-based approach.

Another relevant issue in the prevention and detection of schemes in the procurement cycle is the questionable effectiveness of conflict-of-interest procedures. Junior employees in the purchasing, finance, and accounts payable functions are, at times, made aware of their responsibilities in this area only during the inception of their employment. Even when administered annually, key buyers in many corporations are only subject to a general confirmation of appropriate business conduct. Further, in our experience, annual conflict-of-interest disclosure forms are often collected, but seldom reviewed in more than cursory fashion until an issue arises.

To make these types of confirmation useful as a deterrent, a detailed conflict-of-interest questionnaire that thoroughly addresses the dos and don'ts of procurement risk would be a more powerful control mechanism. Conflict-of-interest disclosure forms are an effective way to set the organization's expectations regarding joint financial interests and outside business arrangements; receipt of gifts, fees, or services; family relations with vendors, etc. Proper administration of these forms makes it more difficult for individuals to collude and conceal their misconduct. Finally, by making it each employee's responsibility to confirm he or she is unaware of wrongdoing, it is more challenging for employees to "look the other way" if they are aware of any issues relating to their colleagues and managers.

Lastly, analyzing procurement trends, payment patterns, and changes in the mix of products and services procured can provide indications of collusive behavior. These analyses require a certain quality of data from accounts payable and procurement, and this is a challenge in itself due to the disaggregate nature of the data and lack of monitoring in place in many procurement organizations.

Differentiating between project scope creep and collusion

The challenge

An international manufacturer of industrial products hired a professional services firm to install an enterprise risk management system, including hardware and software tools as well as implementation services. Senior management became concerned about the constant flow of change orders that eventually grew into a significant percentage of the total project spend and resulted in excessive budget overruns. The problem was exacerbated because the purchaser lacked sufficient technical and operational knowledge to properly oversee this IT project. Careful examination of status reports reflected that unplanned tasks had been inserted into the budget without corresponding changes to the project cost or schedule, especially toward the end of the project's target implementation date. Over time, requirements for this off-the-shelf system evolved and "retro-engineered" into what resembled a custom solution rather than a standard ERM package.

What the organization could do better

Progress monitoring of the project was established during the bidding process, but it was not enforced. The manipulation of the project status reports masked the true nature of the progress made. The company should have utilized a larger team of technology experts to monitor the project budget and milestones. These experts would have challenged the CIO when budget and project milestones were missed by the vendor. Also, the company should have reacted to red flags of scope creep immediately and thoroughly investigated allegations of collusion raised by a disgruntled employee.

Key takeaways

A certain number of change orders can be expected on any large IT project, but when the frequency, volume, and nature of these changes becomes excessive, it's a clear signal that further analysis is necessary by independent resources that have the requisite technical knowledge.

What this means for your business

Addressing procurement risk requires specific attention to its complexities and trends in business environment, policy, and enforcement

Procurement fraud in multinational corporations is complex, technology-driven, and often perpetrated by individuals with significant operational knowledge of the systems they abuse. A common characteristic of procurement fraud that makes detection difficult is that it often takes place over a sustained period of time “under the radar” of management and auditors.

The challenges of evaluating procurement risk are exacerbated by today’s harsh business climate and trends such as rapid consolidation in various industries, globalization, increased use of technology in the payables cycle, proliferation of outsourcing, and an urgency to cut costs. All of these factors make it difficult to maintain effective systems of internal control over the procurement cycle.

For corporations that engage in public contracting, compliance requirements have been strengthened with the recent changes to FAR and by states rushing to enact their own guidelines. It remains to be seen whether the time and effort required to correctly interpret these rules will be prohibitive. Organizations may struggle with language such as “credible evidence” and “timely disclosure,” and given the fragile economic outlook, compliance with the new FAR rules may prove more challenging than anticipated.

On March 4, 2009, President Obama made his position on procurement fraud clear when he ordered an overhaul of the federal contracting system[22] and vowed to “strengthen oversight to maximize transparency and accountability.” To accomplish these goals, a bipartisan effort to establish new federal guidelines on procurement and contracting was launched.

Although the combined impact of developments in public sector contracting is hard to predict, it is safe to expect that while business opportunities in the private sector decrease and public spending increases, more corporations will seek to expand their revenues in the public sector.

As the Obama administration’s economic recovery efforts expand, more contractors and their subcontractors will interact with federal, state, and local government agencies. For many contractors, especially those who were not subject to considerable oversight in the past, the risk of mishandling instances of procurement fraud is likely to grow if they are not carefully monitored. Vendors and contractors in the public and private sectors should take heed by focusing on fraud risks specific to the procurement cycle.

[22] Federal Register, Vol. 74, p. 9755-9757.

Be proactive: Don’t wait until you have a problem

The challenge

A global manufacturer of communications and information technology products learned its processes and controls around contracts and procurement would be audited by the federal government. Not comfortable sitting back and waiting for the results of the audit, the company chose to take proactive measures. It engaged outside specialists and conducted its own comprehensive investigation of its contracts and procurement processes, and several deficiencies were found. The company then implemented a remediation plan and voluntarily disclosed to the government its action plan to immediately address some deficiencies. Results from the government audit mirrored most of the shortcomings uncovered during its own review.

What the organization could do better

Instead of waiting until they were subjected to a series of audits, the company could have implemented an ongoing process to monitor and manage its contracts and procurement processes and controls to avoid last-minute surprises and reduce the need for costly and ineffective short-term remedial action.

Key takeaways

Contract and procurement processes are very complex. They require good controls and adequate performance metrics throughout the entire cycle in order to be effective. The company had to make restitution to the government for some of its deficiencies, but saved money on those deficiencies it remediated prior to the audit. Consistent management and control of these processes is not only cost-effective, but can make a company more efficient and more competitive.

Establishing sound procurement processes and robust controls is an investment that pays off in the medium and long term. Establishing business ethics and compliance programs is a significant step along the path to reducing procurement risk. In addition, the same processes are effective tools when demonstrating that collusion between employees and service providers, fraud by an accounts payable employee, or a kickback received by a purchasing officer are isolated instances that reflect on the perpetrators and not the organization as a whole.

The significance of distinguishing between a rogue employee (or a particular group of rogue employees) and the organization cannot be overstated. Detection of fraud or corruption by management or internal audit is a good indicator that antifraud controls work. Appropriate remediation of rogue employees (suspension, civil and criminal proceedings) speaks volumes about the culture of an organization and can be an effective deterrent. Voluntary disclosure of irregularities in the procurement cycle is expected (and sometimes mandatory) by business partners, federal, state, and local governments and by other organizations.[23]

When allegations arise as a result of a whistleblower complaint or as part of an operational or financial audit in accordance with an audit clause in a contract or under other circumstances, the defense of having a robust system which failed is more powerful than having an ineffective system.

Lastly, addressing regulators', law enforcement's or a business partner's concerns over specific instances of fraud or corruption can be more costly when a corporation is also required to provide assurance that the issue investigated is isolated and not part of a greater pattern of behavior. Reaching a level of comfort that a behavior by a purchasing officer or a procurement evaluation committee is a one-off occurrence often requires deployment of a significant number of resources and evaluation of a multitude of data and transactions. Decisive, transparent, and proactive actions by an organization often prove to facilitate good will and restore trust.

[23] The World Bank Group established its own voluntary disclosure program in 2006.

The bottom line

Corporations should take the necessary steps to establish effective strategies and procedures to prevent waste, abuse, and fraud in the procurement process. The benefits for doing so are clear for companies seeking to close shrinkage and leakage of spend to companies that do business with the government.

For corporations working for federal, state, or local government agencies, the president's announcement regarding overhauling the procurement system and the Task Force and state governments' track records of prosecuting fraud perpetrators serve as clear signs of a coordinated and uncompromising stance on procurement fraud.

When organizations fail to limit both their exposure to and damage from the range of fraud schemes that proliferate in an increasingly complex economic landscape, the consequences—potential debarment, financial losses, public mistrust, criminal penalties, and civil sanctions—are serious. These consequences are avoidable with appropriate, proportionate, risk-based procedures supported by effective actions when required.

"Now, more than ever, there is a solid business case to be made for companies to invest in functioning business ethics and compliance programs, and their clients and customers will demand no less," said Feldman. "Likewise, full compliance with mandatory fraud reporting requirements is going to be essential. Those companies that try to skimp on this, then later face a revelation of wrongdoing that was known internally but not reported, place themselves at a very high risk for suspension or debarment."

Whether by law or economic necessity, companies should increase their focus on evaluating vulnerabilities in their procurement cycle and on the ways they interface with vendors and service providers. Corporate culture and internal controls, which have been scrutinized and revamped in the post-Enron era, must be further refined.

How vulnerable is your organization to procurement fraud?

The checklist allows organizations to assess their vulnerability to procurement fraud by evaluating characteristics that may contribute to a heightened risk of fraud. The results of determining if these statements apply “in most business units or subsidiaries,” “mainly in US and EU business units or subsidiaries only,” or “in a limited number of business units or subsidiaries” can be used as a basis for further discussions among business leaders, risk managers, and legal and forensic resources.

How well do these statements apply to your organization:	Most	Mainly US/EU	Limited
We have a clear policy defining how high-risk vendor relationships are managed including expectations from buyers, personnel in accounts payable, shipping, and IT.			
Our vendors and subcontractors have clear understanding of our expectations and their responsibility in the areas of ethics. We conduct periodic vendor training.			
Our purchasing and procurement personnel sign a detailed annual confirmation that was specifically designed for their respective role and responsibility.			
Our code of ethics includes detailed references to procurement fraud schemes and conflict-of-interest scenarios.			
We perform due diligence/background and integrity checks on vendors:			
- Prior to their initial set-up in our purchasing and AP systems			
- As part of periodical risk assessment of vendors			
We use stratification approach to assess vendors, recognizing that not all high-risk vendors have the same risks and that risk factors change over time.			
We perform a periodical spend analysis across departments and business units that highlights amount of purchases, payment patterns, and frequency of orders.			
We have an effective monitoring of segregation of duties over change order requests.			
We use pilot data to validate assumptions and cost estimates for large contracts.			
Our internal oversight/compliance teams are trained in and focused on monitoring procurement schemes.			
Ongoing oversight and periodic monitoring include surprise visits to vendor offices and project sites.			
We have a controlled, centralized master vendor file process for set-up and maintenance of vendor data.			
We ensure that transfer and maintenance of vendor data between legacy systems (AP, purchasing) are performed while keeping segregation of duties.			
We have a “right to audit” clause for key contracts that allows for independent testing for large contracts.			
Our employees and vendors have access to a hotline that provides local access in high-risk geographies and business units.			
Our training program of procurement schemes is designed and delivered to employees in procurement, finance, project managers, and management.			
Our assessment of procurement risk covers:			
- Analysis of periodical volume of purchases			
- Evaluation of the integrity of the individuals leading key vendors			
- Assessment of compliance associated with signed contracts			
- Analysis of payment terms			
- Integrity risk in international operations			

pwc.com/us/forensics

To have a deeper conversation
about how this subject may affect
your business please contact:

Dalit Stern
Procurement and fraud risk
Corporate investigations
+1 646.471.8047
dalit.stern@us.pwc.com

Phil Treccagnoli
Government contracting practice
+1 646.471.8191
philip.d.treccagnoli@us.pwc.com

Philip Upton
Forensic technology solutions
+1 646.471.7508
philip.upton@us.pwc.com

Brian Delaney
Supply chain management
+1 312.298.3077
brian.m.delaney@us.pwc.com

This document is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. BS 09 0706 0709.