



INTERNAL AUDITORS AND ADVISORS
COMMITMENT, COLLABORATION, CLARITY



Fraud – Whose Problem Is It Anyway?

White Paper

March 2010

Joseph L. Murphy

Managing Director - Quality



Table of Contents

Overview.....	3
Building an effective anti-fraud program – a case study.....	4
Fraud Risk Assessment – What is it? What is the value?.....	6
Fraud Prevention Cycle.....	8
Call to Action.....	12
Final Thoughts	13



Overview

- ***“Fraud Reaches Record Levels in UK”***
- ***“SEC Puts Out Call for Inside Information About fraud”***
- ***“FBI Raids Health-Care Facility in \$14.5 Million Medicare Fraud Case”***

Source: Association of Certified Fraud Examiners (ACFE) Website

Fraud – a five letter word that strikes fear into the hearts of the corporate world. It destroys corporate reputations, wreaks havoc among corporate boards and according to the latest reports issued by the ACFE, costs corporate entities including financial institutions on average 7% of revenues annually. The math is simple, although painful. A \$100 billion corporation is subject to approximately \$7 billion in lost profits annually. An insurance company with a 3% margin would have to sell an additional \$233 billion in additional premiums to recapture lost profits. Corporate fraud costs jobs, opportunities and resources. If 7% of our population was affected with a contagious disease, the Center for Disease Control would have their phones ringing off the hook.

While most corporations have a great need to improve their fraud defenses, the good news is that awareness is increasing. According to a recent survey of Chief Audit Executives, Anti-Fraud Initiatives (sometimes housed under the umbrella of Corporate Governance), consistently ranks among the top five risk management needs for corporations. (Salerno, 2009)

The definition of fraud ranges from such informal verbiage as “Lying, Cheating and Stealing” to the more formal description “Fraud is a false act intentionally, knowingly or recklessly done which is believed and acted upon by the victim to the victim’s damage” . Fraud could take the form of a material misstatement in financial information, misappropriation of assets, and inside dealing or trading. Although there is a standard definition of fraud, identifying a perpetrator is almost impossible as anyone given the right or wrong set of circumstances may feel compelled to commit fraud.

Most organizations have established some form of fraud controls but unless these controls are tested outside of the normal silos of misappropriation of assets or fraudulent financial reporting, the company may still face exposure to fraud. According to FASB Standard AU 316, attest auditors have a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. Fraud affects everyone in an organization and therefore preventing fraud is everyone’s responsibility.

The following is a small sampling of organizations/individuals which have dominated the headlines over the last decade due to the fraud epidemic: Ahold, Tyco, Computer Associates, WorldCom, Global Crossings, Enron, Rite-Aid, Adelphia, and more recently, Bernie Madoff, and Galleon.

Fraud is not new. During medieval times, merchants would sell pigs at market in a bag or a blanket to customers. The customers would often poke the blankets to determine whether the animals were alive (and therefore, the meat fresh) and also to see if there were indications that another animal had been substituted. From this practice, the cliché “a pig and a poke” and “pig in a blanket” originated. Occasionally, merchants would stuff the bags with cats hoping to deceive merchants into believing



that they contained pigs. The bags would occasionally drop and the cats would escape exposing the fraud and giving rise to the saying “don’t let the cat out of the bag.” It seems that rationalizations about fraudulent acts are at least several centuries old.

During the 1930’s, two significant frauds, “the Krueger & Toll fraud” and “the McKesson-Robbins fraud”, shaped auditing procedures that have affected the accounting profession for the ensuing sixty years. This led to an evolving set of standards, pronouncements and regulations that have governed practices by the external audit profession through the 1970’s. In 1977, the Foreign Corrupt Practices Act (FCPA) addressed the issue of bribery of foreign officials and mandated the establishment of a system of internal control for many organizations. The 1980’s saw new focus on the meaning of a financial audit opinion which culminated in the need for a definition of internal control. This resulted in the formation of the Committee of Sponsoring Organizations(COSO) and the issuance of the publication “Internal Control – Integrated Framework” in 1992.

During the 1990’s, the media was consumed with scandals at Sears, Phar Mor Pharmaceuticals, Kidder Peabody, Barings, and Prudential. It seems that fraud takes place in both good times and bad. With the increasing emphasis on short term results, the need to exceed prior period results may outweigh the need to conduct business in an ethical and proper way. Given the impact on businesses resulting from the “Great Recession”, company executives are now faced with severe pressures in consistently being able to report financial results which will satisfy investors and stakeholders in the short term which is often at odds with maintaining the integrity of the financial reports.

In the following pages, we will explore the phenomena of fraud and the ways in which corporations are dealing with this plague on corporate profits.

Building an effective anti-fraud program – a case study

A Fortune 500 corporation decided to update and reinforce its compliance program approximately seven years ago. As part of its’ “Tone at the Top” initiative, a six sigma black belt was appointed to the position of Compliance Director with the intent of putting structure into a program which had been largely conceptual to that point. She began by revisiting the Standards of Business Conduct, researching the key components vs. the guidelines prescribed by the National Association of Corporate Directors (NACD). The following dimensions were examined:

- Risk oversight
- Awareness – including training and education
- Monitoring
- Record keeping
- Governance regulations and reforms
- Communication
- Follow-up and remediation



Year One

While the Standards of Business Conduct were found to be sufficiently comprehensive, a survey of employees at all levels indicated a disconnect between the level of awareness and compliance with those standards depending on geography, business unit and level within the organization. Further, while a third party vendor had been contracted to provide an anonymous employee hotline, the low utilization rate supported the Compliance Director's belief that relatively few employees were aware of the hotline or that most employees did not believe that their identities would be sufficiently protected.

After defining and securing the Board of Directors' agreement on the role of corporate compliance, the Compliance Director embarked on an education program for every major hub within the organization. In the first year, she provided examples of acceptable vs. non-acceptable behavior. She emphasized that her direct reporting relationship to the General Counsel along with the dotted line reporting relationship to the Audit Committee bore testimony to her support by the highest levels of management. She ended year one's education program by pointing out that in using the employee hotline, names did not have to be provided and that a case number would be issued for follow-up and future reference. The use of a third party provider established arms length distance and went a long way in alleviating employee fears of retaliation. Further, the Compliance Director began a monitoring system of calls, delineating them between requests for information and accusations of wrongdoing. If a caller wanted to know the status of their report, they only needed to refer to the case number and the report ID.

NACD guidelines suggest that a successful hotline should reflect calls equaling between one and three percent of the corporate population annually. The Compliance Director began capturing these metrics beginning in year one.

Year Two

Upon completing year one's education program, each business unit and regional management was now responsible for ongoing training. Each plant and major location had a local Compliance Manager who had a dotted line reporting relationship to the Compliance Director. Each local Compliance Manager was responsible for conducting follow-up training annually which was developed jointly with the Compliance Director. Records were maintained of the local training agenda, attendance and test scores. The Corporate Audit Department (CAD) was charged with examining records of attendance during their location visits and reporting back to the Compliance Director on the results. Since the CAD had a follow-up mechanism for all report comments, local management could be held accountable. The compliance survey from year one was redistributed in order to compare progress in year two.

The Company also developed a compliance section on the corporate website that was updated weekly which spoke to current compliance topics and continually reinforced sensitive and important issues on acceptable corporate behavior. In addition, a contract for special investigations was established with an outsourced provider. An action plan was developed once an allegation of wrongdoing was received through one or more of several channels including:



- the compliance hotline,
- letters to board members or senior management,
- direct calls to the compliance director,
- the results of an internal audit, and
- feedback from the external auditors.

A quick response team consisting of the Compliance Director, the CAD director, General Counsel and an Associate General Counsel would determine the best course of action. If specialized skill sets were required for an investigation, the third party investigators were called in. The results of all hotline and potential fraud activity were reported to the Audit Committee quarterly. If controls needed to be implemented in order to mitigate reported or identified control weaknesses, they were included as part of the response.

Year three

At this point, the program was showing signs of maturity having addressed awareness, training and education, feedback, monitoring, recordkeeping, governance regulation and reforms, communication, follow-up and remediation. The annual survey was used as a mechanism for comparison of the program's progress. However, there was still work to be done. A full Fraud Risk Assessment needed to be performed and mapped against the risks outlined in the organizations 10k and by the CAD. The task of fraud prevention is an ongoing battle and this organization has made a commitment to incorporate this initiative into its culture. As robust as these measures were, they did not incorporate a fraud risk assessment.

Fraud Risk Assessment – What is it? What is the value?

A *Fraud Risk Assessment* is designed to be a high impact component to any anti-fraud initiative. Similar to an Internal Audit Risk Assessment in approach, the Fraud Risk Assessment is much more focused and usually characterized by more depth and less breadth than the former. Nonetheless, it is considered an essential element to good corporate governance and a necessary protection for organizations. Fraud exposures must be identified before they can be remediated. For the cost conscious organization, a first step could be a high impact and low cost anti-fraud program assessment tool designed to assist in assessing the completeness of the anti-fraud program when compared against the Committee of Sponsoring Organizations (COSO) integrated internal controls framework and preferred practices.

A *Fraud Diagnostic* includes analysis of the survey findings and the production of a complete, fully integrated report that includes identification of key issues, practical recommendations and suggested actions steps. This provides the auditor and entity management with an indication of current status and what it needs to do to achieve parity with the COSO framework and preferred practices. The opportunity for improvement cannot occur without measurement. This assists the entity to “measure, improve and move” in relation to the adequacy of the anti-fraud program. This approach is also consistent with the principle of continuous improvement that should be built into every organization's approach to implementing anti-fraud programs.



The Fraud Diagnostic does not measure how effectively anti-fraud programs and controls are operating; this should be tested elsewhere by such processes as specific controls testing and data analysis and interrogation.

The Fraud Diagnostic can be completed in as little as eighty hours working time which includes entering findings and recommendations into a reporting template. The elapsed time for the effort will often be longer (e.g. three to four weeks) as documentation will have to be obtained and interviews scheduled. Remember, the diagnostic is designed to provide a snapshot of the entity's anti-fraud framework and not an assessment of how effectively programs and controls are operating.

A Fraud Risk Assessment is much more detailed than a Fraud Diagnostic and involves a series of interviews, surveys and brainstorming sessions which are designed to identify those areas where an organization is exposed to the greatest risk. Often, it begins with the financial statements and the underlying processes which generate activity reflected on the balance sheet and line items.

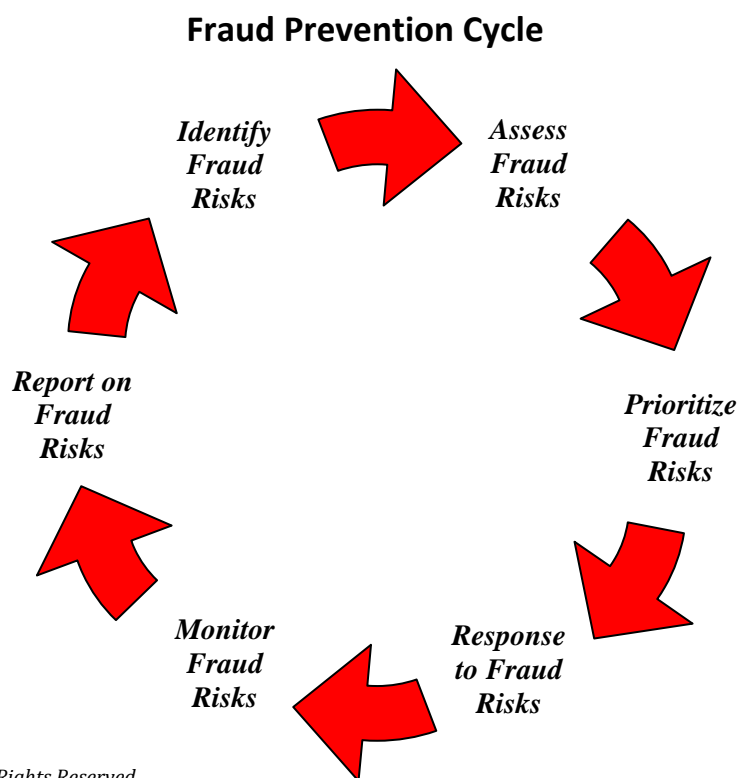
The following is a small sampling of common fraud schemes that represent beginning points for query in a fraud risk assessment:

Misappropriation of Assets	
Cash	Failure to log a transaction in a cash register and pocketing the proceeds
	Using P-cards for personal items with inadequate monitoring controls and supervision
	Misdirection of premium payments
	Theft of incoming checks
Accounts Receivable	Lapping of receivables and misdirecting the checks to personal accounts
	Over-billing
Premiums Receivable	Intentional miscalculation of assumed premiums in reinsurance contracts
Inventory	Misdirecting inventory receipts in an environment which does not perform three way matching of purchase requisitions, receiving documents and invoices
	Misdirecting shipments of inventory, failure to seal trucks and/or failure to reconcile shipments with bills of lading
	Declaring inventory obsolete by the same individual responsible for ordering, receiving and maintaining custody of inventory
	Improper credits, rebates and refunds
	Overriding logistics authorized carriers for shipping (often involves collusion)
Accounts Payable	Personal use of company accounts
	Diverting payments to personal accounts



	Creation of fictitious vendors
Payroll	Creation of phantom employees
	Falsified work hours
Loans	Failure to fully disclose loans to related parties, miscalculation of policy loans (exceeding cash surrender values)
Policy Loans	Miscalculation of policy loans (exceeding cash surrender values)
Improper Financial Reporting	
Revenues	Prematurely recognizing shipments before transfer of ownership has occurred
	Recognizing revenue for goods billed but not shipped
	Recognizing revenue from barter arrangements
	Accelerating recognition of revenues from long term contracts
	Recognizing revenues when disputes exist
	Unsupported adjustments to insurance related reserves (Unearned Premiums, Case, IBNR, etc.)
Expenses	Improperly capitalizing expenses rather than reflecting on the P&L
	Reflecting expenses in the financials of non-consolidated entities
	Recording fictitious or inappropriate amounts for vendor discounts
	Improperly accelerating or deferring expenses

Once the Fraud Risk Assessment is considered sufficiently comprehensive, the key questions asked will surface around the following cycle:



Step 1 – Identify Fraud Risks

This can begin with a simple diagnostic or a more detailed fraud risk assessment. However, if it is less than complete, this should be disclosed to management and any interested parties. The implications of the fraud must also be considered and articulated. For instance, in a life insurance company, if improper premium refunds are a systemic exposure, the reasons and the magnitude of the risk should be evaluated. (e.g. one person processes all refunds, determines the amount and can change the payee with no independent oversight).

Step 2 – Assess Fraud Risks

Typically, a risk assessment will chart a risk into quadrants based on the impact and either likelihood or vulnerability. A fraud risk assessment is no different. In the situation previously described, if there are \$10 mm dollars of premium refunds reflected annually then the following questions should be asked:

- Are all premium refunds properly reflected in the financial statements?
- Are there compensating or mitigating controls in the process which would pick up any refund activity? What is the likelihood that something would be missed?
- What is the likelihood that refunds would be improperly processed, redirected and the magnitude of such an event across the system? Is it material to the overall results?

While these questions by nature are subjective, setting up a range of best, worst and likely is often used in the absence of historical company or industry data. Once all risks are identified in Step 1 and evaluated (or assessed) in Step 2, the results can be tabled as follows:

Risk Components	Scale: 5 High – 1 Low				Mitigating Controls (Satisfactory/Some Improvement Needed/Unsatisfactory)			
	Inherent Risk		Residual Risk		Tone at the Top	Control Activities	Monitoring Controls	Management Override
	Potential Impact	Likelihood of Occurrence	Potential Impact	Likelihood of Occurrence				
New Product Development	5	4	4	3	I	I	U	I
IBNR Reserves	5	4	5	4	U	U	U	U
Claims	4	3	4	2	S	I	I	U
Premium Collections	4	3	2	2	S	S	S	U
Commissions	4	3	3	3	S	I	I	I
Investments	5	3	5	3	S	U	U	U
Treasury	4	3	3	3	I	I	I	I
Sales Practices	5	4	5	4	U	U	U	U
Information Technology	4	3	4	3	S	U	U	U
Regulatory	4	4	3	3	I	I	I	I

Mitigating Controls

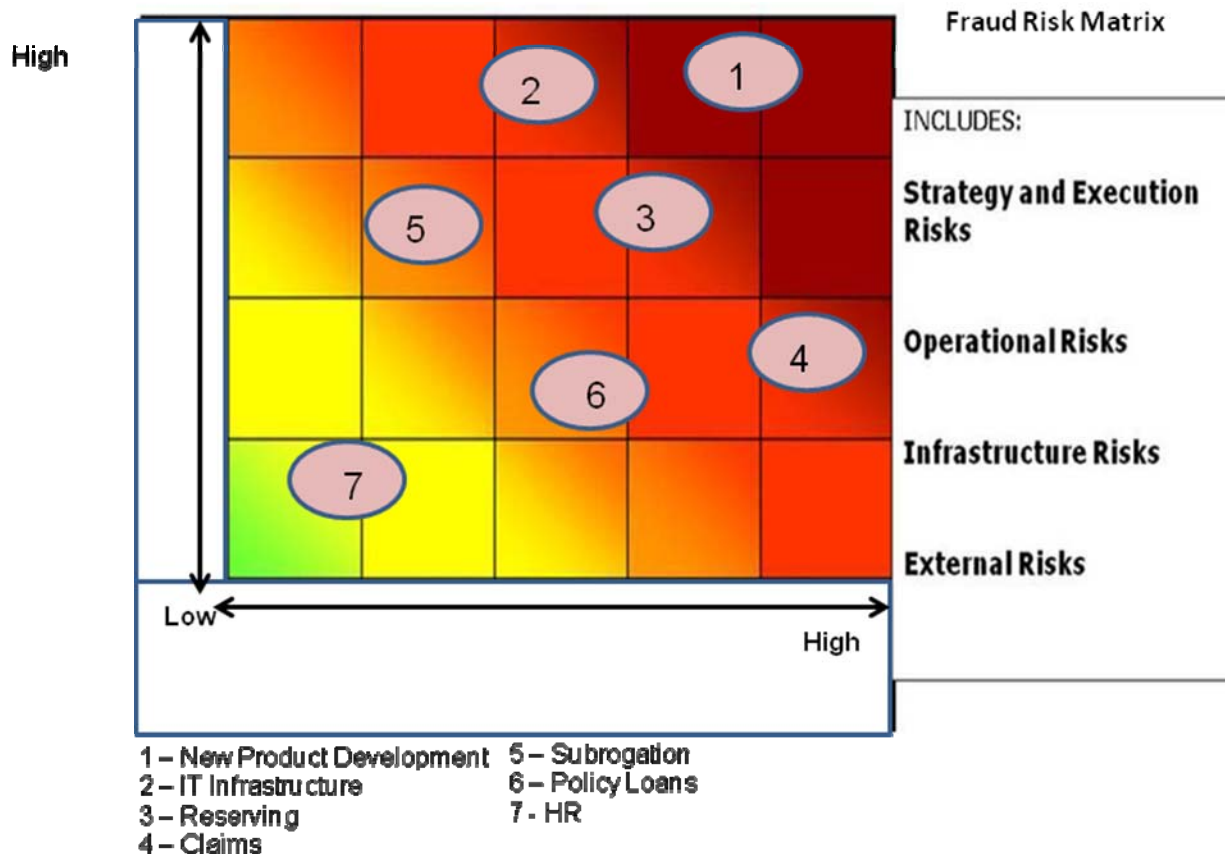
S Satisfactory

I Improvement Needed

U Unsatisfactory



Note that the above chart dissects risks into the raw or unmitigated risks. It then proceeds to factor in any applicable controls and yields residual risks. This is the foundation for prioritizing risks. Ultimately this can lead to graphing in quadrants as follows:



Step 3 – Prioritize Fraud Risks

Once the risks have been fully evaluated, they can be prioritized and an action plan developed. Typically this will be a long term plan which will begin with the items in the upper right quadrant and the “quick fixes”. An additional benefit of using this type of graph is that those items in the lower left quadrant (e.g. low impact and low likelihood) may yield an opportunity for redeployment of resources as these risks may be over controlled.

Step 4 – Respond to Fraud Risks

The key to any risk assessment is to form a basis for aligning corporate exposures to resources. At this phase, the alignment process can begin. If the risks are primarily in the cash controls, process re-engineering or automated controls to prevent diversion of cash assets may need to be implemented. While providing an exhaustive list is beyond the scope of this paper, the process of performing Steps 1 – 3 will identify the magnitude of the effort in Step 4. Preventative controls are always desirable but not always attainable in a cost effective manner. In the long run, The “Tone at

the Top” may, be the most important component in establishing and maintaining an effective defense against fraud. The tone affects the culture and the culture permeates the organization at all levels leading to vigilant and effective detective controls. Most importantly, behavior which is inconsistent with the organization’s standards of business conduct is discouraged. While studies have shown that a small percentage of all individuals act without conscience, the proper corporate tone and culture will reinforce acceptable behavior. While any large organization will suffer fraud due to the law of large numbers, those instances can be limited to the isolated “one off” type situations. By limiting unacceptable behavior in this way, damage to profits, morale and corporate reputations can be minimized.

There are certain instances where the latter two have actually improved depending on the previous variables and the response to actual fraud events. In 1992, a large insurer was fined over \$1 billion for a corporate effort to defraud elderly persons into purchasing life insurance policies which were clearly unsuitable. As a result, the entire industry came under scrutiny by the state departments of insurance. A competitor, guilty of a lone representative using the same marketing and sales practices, offered complete cooperation to two state commissions investigating the matter and was able to substantiate that in the latter instance, the fraudulent practice was isolated. In fact, this action was countercultural to the tone set by management which had a robust infrastructure to deter such acts. The competitor was publicly commended for their cooperation and their high ethical culture. The competitor did not miss opportunities to use this testimony in the marketplace.

Step 5 – Monitor Fraud Risks

In the internal audit profession, the concept of continuous monitoring has been an effort aspired to by many and achieved by few. Continuous monitoring involves establishing key performance indicators around critical processes and establishing upper and lower control limits around those indicators. When one or more indicators exceed a threshold, a warning bell is sounded and questions are asked. In a worst case scenario, a quick response audit or investigation may be warranted. There are many logistical issues to implementing such a system not the least of which is access to data, form of access (manual or automated) and, the homogeneity of the IT platform(s) (e.g. one ERP system or many legacy applications), etc. A more practical solution may be regular, rather than continuous, monitoring. Factors such as changes in personnel, policy, organizational structure, products, past history, geography, and financial performance; when evaluated in light of the current economic environment and public pressures, may present a more effective monitoring system if detailed information is not readily available.

Cynthia Cooper, former Chief Audit Executive at WorldCom, in her book “Extraordinary Circumstances” refers to comments and e-mails made by executives to her directly as the foundation of her desire to accelerate the audit that resulted in uncovering the largest scandal in US corporate history (Cooper, 2008). While technology can be a great accelerator in the search for fraud, most improprieties are still uncovered through the suspicions of co-workers. This makes it all the more important to establish, maintain and reinforce a culture which makes employees believe that they will be encouraged and supported when they do the right thing.



Step 6 – Report on Fraud Risks

Any effective program of fraud deterrence, detection and prevention must include follow-up. All of this activity must be transparent to senior management and the board. While the format and frequency of reporting vary, the message must be simple and to the point. Score carding coupled with a brief narrative can be used to tell the story. An example of a reporting framework is illustrated:

Fraud Risk Factors	Risk	Scheme	Financial Statement Account	Potential Perpetrators	Likelihood	Impact	Controls	Action Steps
Need for improved revenues – Managing General Agents	Withhold claims data from reinsurers	Adjust bordereaus claims data to make business appear more profitable than it really is	Claims incurred and Claims reserves	MGA's, Third Party Administrators	Moderate in a healthy economy/high in a difficult economy	Moderate if not systemic, High if systemic	Reconcile supporting documents at TPA's and MGA's to Reinsurer reports.	Direct link to TPA/MGA systems – enhanced analysis to verify reasonableness of data reported and more aggressive testing at source. (TPA's/MGA's)

If all recognized risks are reported in a manner similar to the above, management and the board should have sufficient information to properly evaluate the potential for fraud.

Call to Action – developing a program to deter fraud

- Develop a Fraud Policy – this should involve at minimum, the Chief Compliance Officer, General Counsel, Chief Audit Executive, CFO, Controller, Chief Risk Officer and the CIO.
- Enhance Audit Programs – this is necessary to ensure that fraud identification, gap analysis and the effectiveness of anti-fraud controls are addressed.
- Leverage Sarbanes-Oxley work – often SOX is performed with SAS 99 considerations in mind. This can also serve as a trigger for additional silos that have not been considered.
- Educate Audit Committee and Boards – many members serve on multiple boards and audit committees and ideas are shared. Why wait for the question on fraud that you know is coming?
- Evaluate Code of Ethics – These should be mapped against the best practices in industry. The National Association of Corporate Directors (NACD) has guidelines for comparison of key issues.
- Provide annual training programs – this is a great opportunity to provide leadership within your organization.

- Integrate fraud monitoring into the Enterprise Risk Management program – this can begin with the financial statements by performing a line item review of areas where your organization may be vulnerable.
- Implement a Whistle Blower Policy – many organizations have already addressed this; non-retaliation clauses are a must.
- Discuss SAS 99 with external auditors – the PCAOB has been addressing this in their review of the Big Four and next tier firms. If your external auditors have not yet approached you, it is a great opportunity to seize the initiative.
- Outside resources – CFEs and consultants offer specialists that can accelerate your path towards establishing an anti-fraud plan.
- Technology – ACL, SAS, data mining and many ERP systems can test 100% of transactions for critical combinations. This can eliminate inefficiencies and reduce manual workload.

Final Thoughts

While the topic of Fraud has many silos, this attempt to portray a high level approach for engaging this threat is intended as a first step to increasing awareness of the magnitude of the issue and the commitment needed to contain it. At minimum, assembling a multi-functional team would be required for first steps. If these skill sets are not present within an organization, seek outside professional advice. The solution can be approached gradually or aggressively but it cannot be ignored. In the Property and Casualty insurance industry for example, the likelihood of adverse occurrences is often characterized in terms of a one in a ten year, one in a twenty year or a one in one hundred year event. As the survivors of Hurricane Katrina found, these characterizations ring hollow if the current year is the one in which the event occurs.

Since preventive action will yield results, all corporate citizens should get the word out and begin an anti-fraud program. Good corporate governance calls for it, rating agencies and regulators are looking for it and our corporate responsibility demands it. Don't delay.

For further information please contact either Joe Murphy (jmurphy@accumepartners.com, Managing Director, tel: 215-499-4239) or Paul Cohen (pcohen@accumepartners.com, Director, tel: 732-682-5074) or visit us at www.accumepartners.com.



U.S. OFFICES

CONNECTICUT

900 Chapel Street
10th Floor
New Haven, CT 06510
P : 203.353.9137
F : 203.782.4329
Paul Nobbs

FLORIDA

6600 N. Andrews Avenue
Suite 278
Ft. Lauderdale, FL 33309
P: 954.938.5670
F: 954.938.5570
Mike Corbin

GEORGIA

3500 Parkway Lane
Suite 290
Norcross, GA 30092
P: 770.446.1539
F: 770.446.3825
Mike Corbin

MARYLAND

5850 Waterloo Road
Suite 140
Columbia, MD 21045
P: 410.480.7099
F: 410.480.7081
Nicole Lloyd

MASSACHUSETTS

225 Franklin Street
Suite 2600
Boston, MA 02110
P : 617.217.2867
F : 617.217.2001
Jim Nabor

NEW JERSEY

341 New Albany Road
Suite 100
Moorestown, NJ 08057
P: 856.914.9500
F: 856.914.9600
Joe Murphy

3040 Route 22 West
Suite 110
Somerville, NJ 08876
P: 908.526.6363
F: 908.526.9944
Paul Nobbs

NEW YORK

80 Broad Street
34th Floor
New York, NY 10004
P: 646.375.9500
F: 646.328.0011
Paul Nobbs

PENNSYLVANIA

4900 Ritter Road
Suite 222
Mechanicsburg, PA 17055
P: 717.796.1650
F: 717.796.7655
Nicole Lloyd

