

Beyond the Recession:Forensic Thoughts

Robert E Farrell, CFE, PI

As we exit 2009 signs are showing that the recession has probably hit its low point, and indicators lead us to believe that the economy is now turning around. The turmoil that has been experienced by companies during this recessionary period has led to near record unemployment due to significant staff reductions, growing concern over the responsibilities and performance of senior management, and increased regulatory and compliance requirements.

As a result, it would appear that businesses would be monitored much more closely as we emerge from this economic setback, but are they? Do these factors ensure a heightened awareness of internal controls, fraud, and abuse going forward? Or do they suggest added risks that must be addressed within?

Take staff reductions for instance. What are the risks that arise from these cutbacks? Fewer people, same amount of work equals more work for fewer people. What happens when time does not allow for the work to get done? What if the system of internal controls is compromised to get work done? What if people end up having to work 50 plus hours a week to get the work done? What if staff feel they are not adequately compensated for the new level of work? What if THEY begin to worry about their jobs?

This plays right into what is referred to as the “Fraud Triangle”; Incentive, Pressure, and Opportunity. These are the three factors that must exist for fraud to occur. Incentive? “I’m doing more work I should get more money”. Pressure? “How can I do all this work?”. Opportunity? “Segregation of duties is impossible with the reduced staff level”. When this happens people will look to take advantage of the situation.

But companies that have implemented a comprehensive anti-fraud program are far less likely to experience surprises than those that have not. Those who have taken the initiative to deal with the fraud risks of the business will safely benefit from their foresight.

Any anti-fraud program must start with effective **Corporate Governance** wherein management sets the tone for ethical behavior for themselves, employees, vendors, customers, and all other third parties who are part of the business and its operations. By instituting and enforcing policies and procedures to safeguard the organization against any illicit conduct by these parties, a message is sent that deviation from these practices will not be tolerated, thereby minimizing fraud risk.

Fraud Risk can be generic and apply to all companies, or company or industry specific relating specifically to an organization or industry. An assessment of fraud risk includes an evaluation of the incentives, pressures, and opportunities that may be present for individuals to commit fraud. Each risk must be examined to determine the likelihood of it occurring and the potential significance of the occurrence. The significance should not only be measured monetarily, but also with respect to the impact on the company’s financial reporting, operations, and legal and regulatory compliance requirements.

Fraud Prevention and Detection are interrelated concepts, but they are not the same. **Preventive controls** are the first line of defense against fraud, and they are the most pro-active elements of prevention. The organization's system of internal controls is the primary element of the fraud prevention process.

Internal controls are mostly associated with the accounting and operational risks of the business. However, additional controls should be designed that include background investigations of all new hires, vendors, and customers; limits of authority; related party transactions; and other areas of concern identified in the risk assessment process. And to be successful, the prevention program must be continuously monitored as to its effectiveness, and changes made when necessary.

Detective controls, by nature, are clandestine. They operate in the background and are not apparent in the daily business environment. The most widely used control of this nature is the Whistleblower Hotline which, when properly installed and operated, provides a broad range of protection among employees, customers, vendors, and others.

Process controls include reconciliations, physical counts, and independent reviews that provide immediate feedback regarding fraud activity. Continuous auditing, utilizing technology on a real-time basis is an essential in today's high tech business environment, and is extremely effective in high volume of transaction type businesses.

This is a brief overview of an anti-fraud program. A comprehensive program involves much more detail, assessment, and design. It is not a program that can be developed by an inexperienced individual. Those that are, are doomed to fail. The work needed to be performed requires a fraud professional trained in the multitudinous facets of fraud and its corollary activities.

As a senior executive, you can imagine from the discussion above where your firm may be lacking in this regard. If your company has been affected severely by the recession, it is probably more susceptible to an event having occurred. If it hasn't, do you feel that you are adequately protected against fraud. Ask your CEO and Board members. What do your Audit Committee members feel?

Could your organization have been the victim of fraud during this period? Is it safe going forward? These are serious questions that need to be answered.