The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 12, No. 10  October 2004

## Project: *Corporate Counsel – Legal Service Providers*

# Fraud Considerations And Internal Control Assessments: What Every General Counsel Needs To Know

**By Kenneth Yormark and David Zweighaft**

Since the Sarbanes-Oxley Act of 2002 (SOA) was signed into law, the halls of executive suites of public companies have seen tremendous activity as CEOs and CFOs address their corporate accountability and financial reporting oversight responsibilities. They now realize that such efforts are more than just good business practice, as they have always been, but also are matters that carry severe penalties under the law. Likewise, audit committee responsibilities have expanded such that membership has become an invitation to delve into a company's affairs at an unprecedented level of depth, subject to the scrutiny of the external auditors as well as investors. This "new era of corporate accountability and responsibility" means that the checks and balances of the system of internal controls are now clearly in the purview of corporate management, including the company's chief legal officer or general counsel (GC).

This shift has raised the bar for many GCs to a higher level of visibility and accountability. For many companies, internal control over financial reporting, especially the related anti-fraud controls, were previously the responsibility of the controller, middle management functions and various process owners, and subject to review and testing by internal audit. The focus has often been limited to third-party fraud. Now that the game has been expanded to fraudulent financial reporting, it requires a referee. Documentation requirements, particularly policies and procedures regarding the anti-fraud program and the internal reporting and escalation of internal control deficiencies, could potentially now fall to the GC to define.

In order to meet the challenges of this significant role in corporate governance, GCs need access to resources and tools that will enable them to make informed decisions when establishing corporate policies and, more importantly, when dealing with situations where there has been a breakdown in internal controls and the possibility of fraud exists. Without proper anti-fraud controls, incidents of fraud can impact a company's financial performance, permanently damage its reputation and result in shareholder lawsuits. All of these circumstances refocus the company resources away from their primary purpose – the operations of the organization for the benefit of the shareholders.

An anti-fraud program and controls are those controls related to the timely prevention, deterrence and detection of fraud. They are the controls that are intended to mitigate the risk of fraudulent actions that could have an impact on financial reporting. Examples include:

- *Fraudulent financial reporting*. Inappropriate earnings management or "cooking the books" – e.g., improper revenue recognition, intentional overstatement of assets, understatement of liabilities, etc.;
- *Misappropriation of assets*. Embezzlement and theft that could materially affect the financial statements;
- *Expenditures and liabilities incurred for improper or illegal purposes*. Bribery and influence payments that can result in reputation loss; and
- *Fraudulently obtained revenue and assets and/or avoidance of costs and expenses*. Scams and tax fraud that can result in reputation loss.

In Auditing Standard No. 2, the Public Company Accounting Oversight Board (PCAOB) clarifies that the focus on fraud, from a financial reporting context, is directed to matters that could result in a material misstatement of the financial statements. It is within this context that management has the responsibility to prevent, deter and detect fraud. The PCAOB also takes the position that deficiencies in the anti-fraud program and controls are at least a significant deficiency in internal control over financial

---

***Kenneth Yormark*** *is a Managing Director in charge of the Sarbanes-Oxley anti-fraud initiative and* ***David Zweighaft*** *is a Senior Manager with Protiviti Inc., a leading provider of litigation support and forensic investigative services, internal audit, and business and technology risk consulting services.* *Parts of this article are adapted from material contained in the third edition of Protiviti's* Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements. *For more information or to download a free copy of this guide, please visit* www.protiviti .com.

reporting. Furthermore, SOA and the revised NYSE and NASDAQ listing requirements, as well as PCAOB Auditing Standard No. 2, place greater responsibility on audit committees to provide oversight with respect to financial reporting and internal control over financial reporting. This oversight extends to reporting, documentation, investigation, enforcement and remediation related to fraud.

The GC's role in this oversight function can be a comprehensive one, starting with reviewing the reporting process and assessing the risks and potential damages should fraud occur within the company, establishing documentation retention policies, articulating escalation policies and processes, and determining when and how investigations should be conducted (including when it is appropriate to engage outside counsel and or other specialists). In addition, the GC should monitor existing policies and procedures for compliance and effectiveness, and determine the appropriate enhancements to meet the company's anti-fraud control objectives.

A key element of any effective anti-fraud program is an anonymous, risk-free means for employees, customers and vendors to communicate any complaints regarding accounting matters, improper conduct of company personnel, management override of internal controls, or any other matters that represent a potential liability to the company (in accordance with SOA Section 301). Typically, this is implemented via a "hotline," and the GC plays a central role in managing the recording, evaluating, investigating, resolution and reporting of these complaints. It is critical to maintain a complete record of all actions relating to hotline complaints, from initial receipt through factual findings, and recommendations for corrective actions, if any.

A common task for GCs in meeting their anti-fraud responsibilities is to engage outside auditors, counsel, fraud specialists or other experts to assist in the investigation of allegations and in the analysis of the results. An investigation may be delegated either within the company or to outside service providers, subject to any necessary confidentiality measures. These activities are consistent with the Amendments to the Federal Sentencing Guidelines (the "Guidelines"), effective November 1, 2004.

Maintaining a complaint hotline is part of the "effective compliance and ethics program" required under the Guidelines, which calls for the entity to "… promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law." Similarly, a GC can reasonably expect to have some involvement in other ethics- and compliance-related activities such as:

- formulating, communicating and enforcing the entity's anti-fraud policy;
- developing or reviewing the content of anti-fraud training materials that are disseminated throughout the entity;
- monitoring and acting upon reported incidents of fraud and ensuring adequate documentation of the entity's actions is maintained; and
- periodically reviewing the entity's anti-fraud policies and procedures to assess their effectiveness and to modify them as necessary to provide continued effectiveness.

In formulating the entity's anti-fraud policy, the GC can provide input as to how a policy can be effective from the entity's perspective and still comply with various laws and regulations, including privacy, human rights and required disclosures. Ideally, policy should be developed as the result of discussions among and between the audit committee, board of directors and individuals with operational responsibility for discrete operating units or processes (e.g., purchasing, payroll, human resources, etc.). As policy is developed, it must be "rolled out" to the entire organization in a manner that communicates management's commitment to preventing and detecting fraud and other criminal behavior. To this end, a message from the GC (or a personal appearance at an anti-fraud training meeting) is a powerful reinforcement to an entity's employees, driving home the notion that the policy is being taken seriously at the highest levels of the organization. Furthermore, a program of incentives should be considered for compliance with the policy, and there should be disciplinary measures meted out for violations.

Once an anti-fraud policy is implemented, the next logical challenge is enforcement of the policy in the case of detected instances of fraud. This is a complex area, frequently requiring that the GC authorize the initiation of an internal investigation to determine the facts and then decide an appropriate course of action (criminal or civil prosecution, termination, restitution, filing an insurance claim, etc.). Oftentimes, the GC may be ill equipped to manage such a process due to time, budgetary or other resource constraints. At the very least, the GC should consider retaining outside counsel and/or other specialists (fraud examiners, forensic accountants and investigators) to assist in conducting a thorough and independent investigation of the matter.

These outside professionals are best suited to assist the entity in fact-finding, analyses and technical activities (e.g., copying computer hard drives, performing massive e-mail searches, reviewing books and records, etc.) that will enable the GC (and outside counsel) to investigate a suspected fraud thoroughly and bring it to a conclusion.

As an entity matures, so must its anti-fraud policy. Over time, employees may develop their own procedures for doing things, some of which may defeat the intent of anti-fraud controls. A dynamic policy is therefore one which can be altered in response to changes in the entity's circumstances and still remain effective. Periodically, the entity's management should assess the risk of fraud or criminal activity occurring and whether the existing anti-fraud policy is sufficiently effective to mitigate that risk. Where it is determined to be necessary, existing policies and procedures should be enhanced to address areas of increased risk. As noted above, the GC should review new or proposed policies for compliance with applicable laws.

In conclusion, the role of the GC in developing an anti-fraud policy as part of an entity's system of internal controls is both diverse and dynamic. The various professional pronouncements and regulatory and legal requirements to which organizations are now subject require input from a variety of sources, both internal and external. Developing policies, communications and training, and monitoring hotlines as well as conducting investigations may become more a part of a GC's role. As GCs find themselves increasingly involved in these areas, it is important to remember that very few organizations address all of them independently and without outside assistance.