The Bulletin

protiviti®
Independent Risk Consulting

VOLUME 1 ISSUE 11

# Establishing an Effective Complaint and Confidential, Anonymous Reporting Process

Last year the SEC issued rules, pursuant to Section 301 (*"Public Company Audit Committees"*) of Title III of the Sarbanes-Oxley Act of 2002 (SOA), requiring audit committees to establish procedures for "(a) the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters, and (b) the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters." Most public companies must be in compliance with this requirement by the earlier of (1) the first annual shareholders meeting after January 15, 2004, or (2) October 31, 2004. Foreign private issuers and small-business issuers must be in compliance by July 31, 2005.

**This edition of *The Bulletin* focuses on the issues that audit committees and management should consider as they collaborate to comply with this requirement. This and other Section 301 requirements are important because the SEC's rules direct the national securities associations to prohibit the listing of any security of a company that is not compliant with them. Noncompliance with Section 301 can also lead to a determination that, at a minimum, there is a significant deficiency in internal control over financial reporting.**

## The SEC's view

The SEC's comments on the new rule refer to the "alleged misdeeds by corporate executives and the independent auditor." In its discussion of the rule for handling reports of such matters, the SEC states:

> ... we are not mandating specific procedures that the audit committee must establish ... We do not believe that in this instance a 'one size fits all' approach would be appropriate. .... We expect each audit committee to develop procedures that work best consistent with its company's individual circumstances to meet the requirements in the final rule ...

The Commission acknowledges that audit committees must rely on management for information about the company's financial reporting process. Further, it states that the establishment of formal procedures for receiving and handling complaints should serve to facilitate disclosures, encourage proper individual conduct and alert the audit committee to potential problems before they have serious consequences.

## A state of flux

While many audit committees are modifying their charter to insert verbatim the language from the statute as a "working model," few committees have addressed specifically how the process will work. As a practical matter, whistleblower complaints, whether financial or legal in nature (or both), can present sensitive situations for directors and management. One concern of many executives is that it is not unusual for complaints to come from irresponsible or aggrieved employees. For example, multinationals have experienced disgruntled employees claiming knowledge of violations under the Foreign Corrupt Practices Act.

While this area is in its infancy, an analogy can be made to other situations requiring director follow-up. For example, in the event a board receives a responsible allegation that a member of management has engaged or is about to engage in a material, unlawful act, how is it required to act? In such instances, directors often take a conservative approach. They may require and oversee a comprehensive investigation, listen to the complainant (if he or she will come forward), seek advice and formal recommendations from outside advisors and counsel about appropriate board or committee action, formulate a final decision, take action in accordance with that decision, and if necessary, make appropriate disclosure inside and/or outside the company. Complicating this process, however, is the SEC's recent "up-the-ladder" rules for legal counsel to "blow the whistle" for inadequate disclosure or breach of fiduciary duties. These rules raise questions for management as to the appropriate process for consulting counsel for advice on handling matters reported by whistleblowers.

## Some practices to consider

Section 301 differs from other SOA requirements in that it states that the audit committee "must establish" the procedures required to handle complaints and confidential, anonymous submissions. To fulfill its responsibilities under the statute, the audit committee needs help from management, counsel and advisors with the design and execution of the appropriate process. If management is proactively and effectively addressing these requirements, the audit committee's approval should be sought. The committee should provide input as to the appropriate protocols (see below) and oversee the process to ensure those protocols are honored. The process must consider how to assess these matters, determine who will investigate them, and address how results will be communicated to management and the audit committee.

Some process design points to consider are discussed below:

- Design the reporting process to use, considering the company's culture, structure, complexity and risk profile. An employee

whistleblower program is a process available to employees designed to allow them to report complaints and concerns on a confidential, anonymous basis. The procedures that will be most effective to implement such a program for, say, a small company with 100 employees could be very different from the processes and systems that would need to be in place for a large, multinational corporation with tens of thousands of employees. Many organizations use "employee hotlines" that allow employees to call toll free and report incidents and complaints on a confidential, anonymous basis. *The idea is to design and promote a program with the goal of enabling employees to have a dialogue about potentially serious issues in a manner that they respond to favorably.* While hotlines are effective tools for addressing the Section 301 requirements, they are only one piece of the puzzle.

- Develop appropriate protocols. Protocols are needed in several areas. For example:
  - *Reporting protocols* define (a) how complaints are received and by what facility, i.e., by an external hotline vendor or through internal staff, (b) where the complaints go when they come in, and (c) when complaints warrant immediate escalation to the audit committee. All reported complaints should be documented and sent to the audit committee on a periodic basis, e.g., monthly or quarterly. Serious matters, however, should be reported to the committee as soon as possible.
  - *Complaint cataloguing protocols* provide guidance on categorizing and prioritizing complaints and submissions to facilitate subsequent review. Filtering is a significant part of the process. The task is to segregate complaints, anonymous or not, having relevance to accounting, internal accounting controls, auditing or fraud matters so that they are reported in an appropriate form, including in a summary report, to the audit committee.
  - *Investigative protocols* facilitate decisions to investigate matters as well as ensure privilege, confidentiality and appropriate communication of findings. They include, among other things, (a) determining whether complaint handling is free of conflicts of interest (i.e., reported issues may concern an investigative team member's area of responsibility), and (b) ensuring use of appropriate evidence-gathering techniques to facilitate admissible characteristics. These protocols are important in any fraud investigation that may result from a complaint.
  - *Protective protocols* address the specific SOA Section 806 provisions that protect whistleblowers. Employees who report accounting irregularities and fraud must not be singled out or discriminated against because of their actions.
- Develop a communications strategy. With assistance from management and advisors, the committee should formulate a comprehensive plan to announce the procedures for handling complaints and submissions to all company employees. The goal is to ensure all employees recognize that they should report any fraudulent or unethical behavior. Periodic reminders on the process should ensure employees understand the importance and parameters of the program and follow its guidelines. For example, consider:
  - Incorporating the complaint hotline information on pay stubs and websites
  - Communicating the information during regular performance feedback, consistent with the company's human resources program
  - Providing a strong education component to improve the quality of reported data as well as ease the filtering process
  - Incorporating a clear articulation of the consequences for abusing the complaint system, including dismissal
  - Including information in new employee orientation and periodic training programs to ensure all employees, regardless of their position or status, are aware of the process and the related protections
- Determine the makeup of the complaint assessment team. The assessment team should be led by the general counsel and should include the chief compliance officer and a senior representative from human resources. If there is one, the chief risk officer, the ethics officer/ombudsman and chief security officer should be included. Each complaint should be investigated with appropriate documentation. Depending upon the nature and complexity of the complaint, appropriate audit techniques and a review of IT systems logs may be important to a proper investigation, requiring the participation and assistance of the internal audit director and chief information officer. Highly sensitive complaints will need to be investigated under the direction of the audit committee. In these instances, the audit committee should consider having the investigation coordinated by outside counsel. Other complaints may be delegated to management with accountability for reporting back to the committee. The audit committee must be satisfied with the resolution process.
- Identify and establish a relationship with appropriate advisors and auditors. The committee should consider the assistance it will need from management and advisors with designing the process, defining the protocols, developing a communications plan and, if necessary, conducting investigations. The committee should engage outside counsel to advise on legal and reporting matters. The committee may want to identify outside forensic accountants and independent investigators and establish a "go to" relationship with these parties. Relationships with and assistance from local and federal law enforcement agencies may also be considered to ensure timely participation, if needed. Guidelines are also needed for communicating with the outside auditor when conducting an investigation. Depending on the nature and type of investigation and the status of the investigation, the committee may need to inform the external auditor of the complaint or anonymous report. Remember, Section 302 of SOA requires management to disclose to the external auditor (and audit committee) any fraud, *regardless of materiality*, involving someone who is a participant in the financial reporting process. Thus management must be appropriately involved.
- Maintain good records. Records should be kept of meetings, actions taken and the results of those actions, including the disposition of all complaints, whether investigated by management or the audit committee. These records should include a summary of the facts, recommendations and resolutions and, where appropriate, the committee's conclusions and direction to management. Required actions may include process changes, disclosures, employee training, fraud-prevention efforts, risk-assessment activities and terminations.
- Conduct a fraud risk assessment. While listed last, this suggestion could just as easily have been listed first. A fraud risk

assessment with senior and possibly middle management can identify accounting- and fraud-related risks within the organization. Such assessments often provide insights as to patterns and common industry issues to watch for when evaluating complaints and submissions. They may also identify areas where a proactive solution is warranted to minimize the risk of fraud. Following are steps to consider when conducting a fraud risk assessment:

- Understand the company's industry specific and geographic fraud risks. For example, determine if the company operates in countries where corruption and fraud risk is high. Certain industries also have unique fraud risks, and the risk assessment should identify these factors.
- Review all previously issued reports concerning fraud. Internal sources or external consultants may have issued reports regarding fraud issues that may still be relevant.
- Evaluate the existing anti-fraud program and related policies. The program should have elements of prevention, deterrence and detection. Determine if there is corporate oversight of the anti-fraud efforts to ensure consistency throughout the organization.
- Consider conducting facilitated meetings with various management personnel to determine their perspective on fraud within the organization. These meetings should include representatives from senior management and the business units. They should also include corporate functional heads such as finance, human resources, risk management, corporate security, information systems and internal audit.
- Conduct surveys of other employees to understand their knowledge of the frequency of fraud. Utilize web-based survey tools to reach the greatest number of employees. Use these surveys to determine if employees understand the company's fraud prevention, deterrence and detection policies.
- Compare findings to those of similar organizations. Search for best practices rather than just benchmarking against peers. "Think outside the box" and find the best solutions for your company.

## Getting started

While the audit committee has the ultimate responsibility for making decisions regarding the nature of the process, many companies are not starting with a "clean slate." A practical step is for management to provide information about existing procedures so the committee can evaluate their suitability for purposes of complying with the statute. Many large organizations have established procedures to investigate the various types of complaints, including conflicts of interest, violations of law, fraud, theft and misuse of assets. The audit committee, with the assistance of its advisors and management, should evaluate the scope and adequacy of these processes if they exist, and request modifications of them, as necessary, to meet the intent of SOA Section 301. Alternatively, the committee should ask management to submit a plan for the design and implementation of an appropriate process.

Following are examples of things the committee should request for the last three years at a minimum:

- Any consultant studies regarding the code of conduct, ethics, compliance, anonymous reporting of complaints, fraud prevention, etc.
- The existing code of conduct, compliance procedures, internal documentation of fraud, fraud policies, etc., and any recent changes or waivers
- Any completed risk assessments indicating the possibility of accounting irregularities or fraud to understand what was recommended and how management responded
- External audit management letters or internal audit reports that address sensitive matters

If a confidential, anonymous reporting procedure is already in place, the audit committee should request information about current policies and practices, how the process works, who receives the initial complaint, how the complaint is forwarded to management and how the company normally handles complaints. The audit committee's purpose is to assess whether the established process can accommodate accounting, fraud, ethical and conflicts-of-interest issues. If there is a process for investigating sensitive complaints, the committee should obtain information on the composition of the investigation team, who determines when to investigate, and typical investigatory scopes, approaches and reporting. The committee should also understand from management the historical frequency of fraud incidents and ethical violations. If a hotline is in place, the volume of use is an indicator of its operating effectiveness.

The committee should consider conducting executive sessions or interviews with appropriate executives to gain their perspective on historical issues and incidents. These executives may include the chief financial officer, internal audit director, general counsel, chief human resources officer, chief compliance officer, chief risk officer, controller, ethics officer/ombudsman, business unit heads and external auditor.

Over time and with the assistance of management, the committee should find out what other companies are doing. Through input from advisors and networking with other directors and executives, obtain examples of practices on complaint reporting and the related management processes. Evaluate these practices as they apply to your industry and to your company's facts and circumstances.

## Managing the process

When managing the process going forward, audit committees will require assistance from management, staff and advisors. Ordinarily management will provide a plan for the committee to approve. The plan should specify the level of effort required of management, support staff and outside advisors. Note that Section 301 of SOA requires companies to fund the outside advisors the audit committee deems necessary.

The audit committee must pay close attention to any sensitive investigations it initiates. When overseeing such investigations, it is imperative to understand "what to do" as well as "what not to do." For example, an investigation's objectives must be clearly articulated. It must be conducted in a comprehensive and objective manner. Equally important is determining if and when the findings should be reported and to whom and how. While investigations are underway, information should be restricted to those individuals designated by the audit committee as having a "need to know." Failure to conduct internal corporate investigations on a discreet basis can result in embarrassing leaks. Further, if not gathered and preserved properly, evidence may be considered inadmissible in a court of law, creating further embarrassment. Often, in these types of investigations, an

employee's career may be on the line, so every attempt must be made to be fair and to limit the release of any potentially damaging information. Someone who has experience conducting sensitive, "board-level" investigations should lead the investigation team.

Sometimes organizations take disciplinary action against an employee before completing an investigation. Making rash decisions based on emotion and without all the facts can lead to mistakes. Conducting an investigation after disciplinary actions are taken can compromise the objectivity of the inquiry.

Another factor in managing the process is employee law, which varies by country and, in some cases, by state. In some countries, investigations must be completed within a specified time period once management determines there is cause for an examination of the facts. In addition, some countries may require the participation of employee "works councils." The process must ensure timely review of the facts, determine if an investigation is needed and drive decisive action.

### Using "hotlines" for confidential, anonymous reporting

While the SEC does not specifically require the use of an external-based hotline, audit committees and management may wish to investigate the firms offering them. Considering the inherent complexity of managing sensitive information and responsive investigations, it may be both more cost effective and free of conflict-of-interest issues if third-party providers supply the primary complaint hotline facility and collect information through that facility.

Hotlines have been around for a long time. They were first established within the retail industry to allow sales associates to report theft, shoplifting and pilferage. They proved to be an efficient way to reduce shrinkage. In the past, organizations have used hotlines to receive complaints regarding racial and gender discrimination, sexual harassment, and government contract fraud and abuse. If administered properly, they also allow for reporting of accounting, internal control and auditing deficiencies as well as fraud, and can provide a deterrent that can reduce the number of reported incidents over time. An independent third-party normally administers hotlines to maintain confidentiality and anonymity.

Some new service providers offer their clients the opportunity to implement Internet-based reporting of complaints. In lieu of external providers, some companies merely utilize *internal* phone numbers that receive voice-recorded complaints from employees. Internal hotlines may be used by the audit committee so long as they are accessed and managed by a company employee (a compliance or ethics officer, for example) who reports directly to and works directly with the committee. These options have advantages and disadvantages that must be considered carefully. For example, one of the clearest benefits of an external provider is that the reporter will not be speaking with someone he or she knows. Another issue is to understand the distinction between "anonymity" and "confidentiality," as they are not one and the same. If the intention is to promise anonymity, the process must be designed to preserve it. Once the source is known, anonymity is lost for good.

Hotlines are only a tool and are not the whole solution. It is possible that the organization may already have one or more internal hotlines in play. If there are too many hotlines, employees can get confused. Thus the audit committee needs to carefully weigh its options before deciding to go forward with a new hotline.

### Some things to do and avoid

In closing, the SEC's rules on complaints and confidential, anonymous submissions set expectations for compliance without cumbersome details regarding methods to use. Protiviti has developed a checklist of important things audit committees and management should consider, with the assistance and support from counsel and advisors. The checklist also includes mistakes to avoid. The checklist, entitled "Some Things to Do and Avoid," is available as a supplement to this issue of *The Bulletin* on **www.protiviti.com**.

## Key Questions to Ask

### Board members:

- Has the audit committee begun the evaluation of the design of the processes to handle complaints and confidential, anonymous submissions by employees and others concerning accounting, auditing and fraud matters?
- Has the audit committee solicited the support of and obtained input from management in designing this program?
- Has the audit committee sought out advice regarding the reporting, cataloguing, investigatory and protective protocols necessary to make the program work?
- Is the audit committee using the staff and advisors it needs to design a compliant program, receive and catalogue complaint submissions, decide complaints to investigate, conduct investigations, evaluate and report investigation results, take corrective action where necessary and maintain adequate documentation (including committee minutes) of the activities?

### Management:

- Has management recommended approaches to the audit committee for the complaint and confidential, anonymous reporting process, including consideration of existing processes and reporting mechanisms?
- Is the company in compliance with the Federal Sentencing Guidelines? How do you know? (For more information on the Federal Sentencing Guidelines, please refer to the supplement to this issue of *The Bulletin* on **www.protiviti.com.** )
- Has the company documented its history of accounting irregularities and fraud incidents so they can be reported to the audit committee?
- Has the company conducted an assessment to understand the unique risks – particularly those relating to fraud – within the organization, the industry and the various geographies the company operates?