SecurityManagement
As Seen in the February 2004 Issue

FINANCIAL SERVICES

New laws hold top executives directly responsible for making an earnest effort to prevent fraud and ensure that financial disclosures are complete and accurate.

The Importance of Being Earnest

By Howard Silverstone, CPA

The Sarbanes-Oxley Act, passed in the wake of Enron and other scandals, seeks to reduce the likelihood of fraud by making public company CEOs and CFOs directly accountable for their organizations' internal controls and financial disclosures. Senior managers will also be subject to greater oversight from more independent boards, internal audit committees, and external audits. Rather than looking on the new law as imposing onerous requirements, however, management should view it as an opportunity to take a fresh look at the company's internal controls, to assess its risk of fraud, and to make changes where needed to reduce the organization's overall exposure to loss. The new emphasis on internal controls also offers corporate security the opportunity to become more involved in helping management prevent and detect fraud.

The goal of the new law is for internal controls to be so effective that degradation of the system through fraud is virtually impossible. While it can be argued that fraud can never be eliminated, the onus is on management to create the most effective system possible to prevent it and catch it. Audit firms will be asking hard questions to see that this is so before certifying any management report, since their own review must withstand subsequent scrutiny by the Securities and Exchange Commission (SEC).

Audit committee. What does a system of Sarbanes-Oxley-compliant controls look like? The first step to compliance is the establishment of an audit committee. Every public company must have one. The members of the audit committee all have to be members of the board of directors but independent in the sense that they perform no other corporate duties and receive no other compensation than their directors' fees.

At least one member of the audit committee must be a "financial expert." (The SEC will judge the level of expertise based on previous responsibilities, education, and experience with internal controls and the preparation of financial statements.) The audit committee is responsible for hiring and compensating both the auditors and any other consultants and is thus the logical body to oversee the entire compliance process from review through to implementation.

Since audit committee members are drawn from the board of directors, a company may first need to revamp the board so that it can supply the financially experienced, independent members required by Sarbanes-Oxley. Although not spelled out by Sarbanes-Oxley, a significant control issue to be questioned by the external auditor will be the level of experience of the individuals on the board. Directors should be experienced businesspersons, and as many as possible should be directors on other boards.

Another concern is whether board members have inappropriate ties to the company. A report, *Fraudulent Financial Reporting: 1987-1997: An Analysis of U.S. Public Companies,* published in 1999 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, found that about 60 percent of the directors of fraudulent companies were insiders or so-called "gray" directors; that is, they had a high level of equity interest or some other personal or business connection with the company.

Sarbanes-Oxley states that audit committee members cannot be "gray" directors. Close family relationships among directors or the concentration of power in too few hands will also have to be questioned by the external auditors. Sarbanes-Oxley is trying to make the charismatic CEO with a compliant board of inexperienced family members and cronies a thing of the past.

The audit committee must have the authority and resources to carry out its duties. As a rule, the committee should be active without being meddling. A written charter should set forth the meeting calendar, manner of reporting to the full board, plans for conducting the audit, role of legal counsel, selection process for the external-audit engagement, expense and compensation policy for the committee, and any other relevant matters. This charter should always be developed with the assistance of management.

It may seem simple and obvious, but the external auditor will certainly ask about the frequency of audit committee meetings. The 1999 COSO report found that the audit committees of companies concealing fraud usually met only once a year. Once every quarter should be the minimum.

Since the separation of the audit and accounting firm consulting functions is one of the key elements of Sarbanes-Oxley, the audit committee should be especially aware of all

consulting engagements and make sure that there are no conflicts of interest. The committee should also act to ensure the total independence of the external auditors and review all consulting and external audit fees.

Committee members should be prepared to question management on any unusual transactions or novel practices. The committee should also discuss with the external auditor any questions the auditor discussed with management, and it should not be afraid to demand answers to any of the committee members' own questions.

The audit committee should be especially vigilant in exercising its oversight authority if, after a disagreement with the auditors, management seeks a second opinion or requests a change of auditor. Genuine differences of opinion among accounting experts do, indeed, occur. Sometimes, however, management may be seeking a favorable opinion to ensure its bonuses or slip a fraudulent transaction past the auditors. Audit committee members must exercise the full force of their experience, impartiality, and knowledge in these difficult cases.

The chair of the audit committee should, as a matter of policy, keep an open door for the chief internal auditor, the security director, and the CFO and have good communications with the engagement partner of the external auditor. Since the Sarbanes legislation, many companies have also set up "whistleblower hotline" services, which let their employees use various communication methods (such as voicemail) to report suspected incidents and hold confidential discussions with members of the audit committee. A receptive and cooperative attitude means early knowledge of trouble and quick response time. Problems can never be allowed to fester because the chair of the audit committee appeared unapproachable.

Code of ethics. The next step should be the establishment of a code of ethics, which must apply equally to front-line employees and senior executives. Of course, a code of ethics is only as good as the willingness of employees to be governed by it; no code can stop a person determined to commit fraud. But criminologists have shown again and again that employees who commit fraud are not hardened criminals; rather, they are average people who, faced with either temptation or financial crisis, will turn to fraud if the opportunity arises.

Good internal controls can help to reduce the opportunity for crime (more on this later). But the corporate culture also plays a role. Employee attitudes are shaped to some extent by the attitudes of senior management. Where management is seen to be adhering to the highest standards of business practices, employees are more likely to do the same. Thus, the role of the code of ethics is to set the right tone and to dissuade good people from making the wrong choice in their moment of weakness or crisis.

Sarbanes-Oxley recognizes this moral responsibility of senior management and the audit committee. Sarbanes-Oxley requires any code to focus on conflicts of professional and personal interest, full disclosure of relevant matters in the company's regular filings, and compliance with government rules and regulations. This section seems aimed at preventing a repetition of improper insider trading. The code of ethics should be written and thoroughly explained to all levels of employees.

The author knows of one company that has its code of ethics in five languages available at its Web site and on paper not only to guide its employees at all levels but also to be read by shareholders, customers, and suppliers. The code discusses the main issues of concern such as conflicts of interest, fraud, gifts, harassment, proprietary information, e-mail, and insider activities. The highlighted topics are followed by generic examples to illustrate the principles involved.

Internal controls. Another requirement under the new law is that management identify and assess the risk of fraudulent financial reporting within its own operations and the adequacy of internal controls. That means reviewing the existing environment as a starting point. This review should have the character of what has become known as a forensic audit. During such an audit, the company, typically with the assistance of expert consultants, looks for weaknesses and opportunities for fraud.

It should be noted that a review cannot be avoided simply by pointing to a recent clean audit opinion. That opinion is irrelevant so far as Sarbanes-Oxley is concerned, because the traditional audit was never designed to review internal controls in the manner now expected. Nor can management sit and wait for the external auditor to tell it what is needed, because setting up the system is management's responsibility. Only after these steps have been taken will the external auditors attest to and report on the assessment made by the management team.

The goal of the new law is for internal controls to be so effective that degradation of the system through fraud is highly unlikely.

What exactly might good internal controls entail? COSO's seminal 1987 *Report of the National Commission on Fraudulent Financial Reporting* (known as the Treadway Report) looked to the Federal Corrupt Practices Act of 1977 for a definition of what assurances an effective system of internal controls should provide to ensure that transactions are not fraudulent. It said that transactions must be authorized by management and recorded in such a way as to permit preparation of financial statements and an accounting of assets. Only management should be able to authorize access to assets, and a physical count should periodically be made and compared with the record.

But just having management oversight is not sufficient. The 1999 COSO report on fraudulent financial reporting found that of the nearly 300 cases studied, the CEO and CFO either alone or in collusion were associated with 83 percent of the frauds. These cases show how important it is for the responsibilities of the senior officers to be strictly segregated. For example, the CEO should not act as the CFO. Spending limits and signing authorities must be clearly defined.

Of course, the real question is how well these controls are enforced. Unfortunately, studies of fraud cases brought to the attention of the SEC

between 1981 and 1986 showed that the executive power to override controls was also a consistent factor in frauds. The Association of Certified Fraud Examiners has also found in its research that the opportunity for executives to override controls is a serious threat. This threat must be addressed by each company in the context of its own corporate structure.

The expanded role of the audit committee is intended to help address this issue. Although it varies from company to company, the audit committee's role as to internal audit and monitoring of CEO/CFO activity must include a review of the effectiveness of internal controls and the internal audit function. The committee must also review management and the company's code of conduct at least annually. It is one thing for the company to have a code of conduct; it is another for management to review it regularly and enforce it.

Internal audit. An effective internal audit function with adequate staff is an essential part of any internal control system. The internal audit team should have the full support of senior management, the board of directors, and the audit committee.

The integrity and impartiality of the chief internal auditor and the members of the team should be beyond question. The chief internal auditor should report to a senior officer not involved in the production of financial statements and should have direct access to the CEO and the chair of the audit committee at all times.

The internal auditor brings a detailed operational knowledge that should be coordinated with the work of the external auditor to develop antifraud controls. Companies must not become overly reliant on the internal auditor to detect fraud, however.

Of the 663 known fraud cases studied by the members of the Association of Certified Fraud Examiners for its 2002 report, internal audit teams were responsible for discovering only 18.6 percent, while mere chance turned up 18.8 percent. Notably, tips from employees revealed 26.3 percent. Thus, the internal audit must be seen as only one of the internal antifraud controls. Honest employees inspired by ethical business practices and protected by new whistleblower legislation under Sarbanes-Oxley should be encouraged to play their role as part of the internal control system.

Fraud prevention and detection is where corporate security can have the greatest impact. For example, many security professionals are responsible for internal investigations of suspected fraud and for making recommendations to internal audit regarding improvements in safeguarding assets. Corporate security also may be responsible for setting up and overseeing an employee hotline.

Common problems. The most common problems that the author has encountered when reviewing clients' internal controls since Sarbanes-Oxley became law involve failure: failure to segregate conflicting duties, failure to reconcile accounts, failure to have these reconciliations reviewed by someone independent of the reconciliation process, and failure to do follow-ups to make sure problems get solved.

These problems are uncovered in some cases when the company itself recognizes that a problem has occurred that must be fixed before senior management and the external auditors can attest to the effectiveness of internal controls; that leads to an outside review. In one case, for example, a distributor had been growing rapidly through the acquisition of distribution centers in several states. After a year or so of expanded operations, an unexplained inventory shortfall in excess of $30 million was discovered during a routine internal audit.

Detailed interviews with accounting personnel in the home office and at the newly acquired companies showed a range of perceptions as to how intercompany transfers were to be handled. A $20,000 transfer from inventory would be recorded as $20,000 in internal sales; however, perhaps only $15,000 worth of inventory was actually shipped and recorded as a $15,000 intercompany payable by the recipient. No one had called to check that the amount actually received was the amount sent or to question why there was a discrepancy.

By the time my firm was called, millions of dollars of inventory needed to be reconciled and explained. So many problems had been outstanding for so long that management could not tell whether arithmetic errors, sloppy recordkeeping, or fraud had created the discrepancies.

We recommended tighter inventory controls, more frequent communication between the shipping and receiving companies, and better documentation in the form of shipping and receiving slips. Reconciliations are now made monthly and any differences are investigated and reconciled at once.

Another company had experienced several embezzlements, and while management believed the problems were behind them, it chose to have an independent examination of its internal controls to satisfy the audit committee. We found that the problem had concerned one employee in the accounting department who was making the most of conflicting responsibilities. She not only received the bills from suppliers but also had the authority to generate manual checks to pay them.

Since no one was reconciling the bills with the checks, this employee created a few false accounts and wrote checks to herself. After the fraud was revealed, the company introduced a more effective reconciliation process, imposed another layer of oversight, and generated all checks by computer.

In the 18 months following the discovery of the fraud, the company had made great strides in tightening its internal controls overall. During the same period, the company had expanded, creating potential problems because some of the company's accounting functions were being conducted at the home office, while many others were decentralized.

That arrangement had advantages and disadvantages. The biggest advantage was that collusion to commit fraud would be very difficult. The challenge for the company, however, was to maintain a balance of decentralization and control without making the reporting process so time consuming that people would try to circumvent it.

Many companies face that same challenge as they seek to develop good internal controls. The bottom line under Sarbanes-Oxley is that whatever approach it takes, top management will now be under the watchful eye of more independent boards and external auditors—and will be held directly accountable for the company's financial statements. ■

Howard Silverstone, CPA, FCA (Fellow of the Institute of Chartered Accountants in England and Wales,), CFE (certified fraud examiner) is a principal with Kroll Inc., in Philadelphia.