Internal Control at Private Companies and Nonprofits

Using SOX to Your Advantage

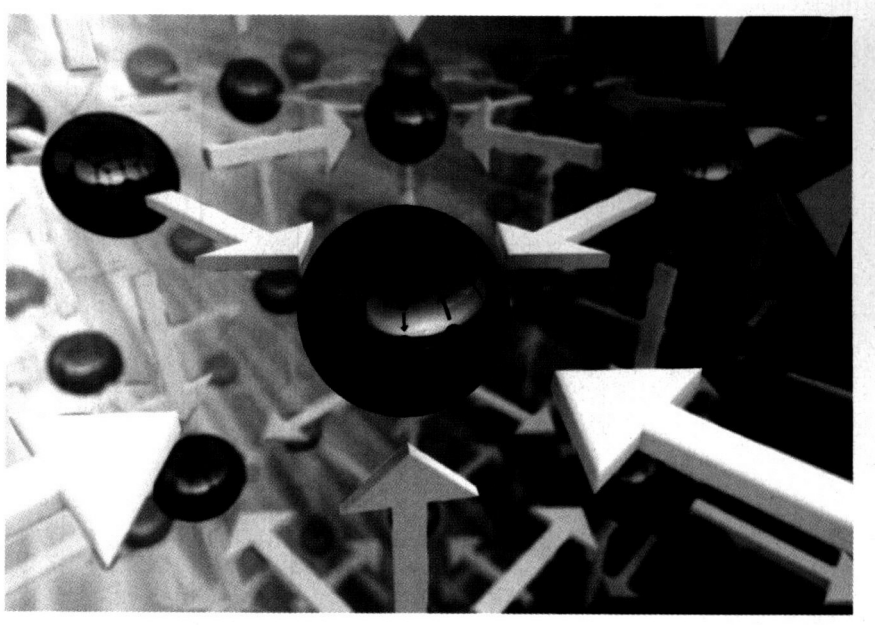
By Chris Jeffrey

Should the Sarbanes-Oxley Act (SOX) be applied to a private company? What about SOX at a nonprofit? Over the past few years, it has become evident that the strong corporate governance and systems of internal controls put in place by SOX are here to stay. It has become clear, through the actions of regulators, the market, and individual companies, that an active and vigilant board of directors, an effective system of internal controls, and a control-conscious environment are essential to the viability and health of any organization or institution, whether publicly traded, privately held, operating as a nonprofit, or located domestically or internationally.

Of course, since the passage of SOX, corporate governance—or more specifically the method by which to achieve successful corporate governance—has been under fire. The SOX mandate for SEC registrants has been criticized as being too costly and burdensome, especially on smaller organizations. In the final report of the Advisory Committee on Smaller Public Companies (a committee established by the SEC to assess the current regulatory system for smaller companies under the securities laws, including the impact of SOX), the committee reported that the costs of SOX compliance ranged from 0.06% of revenue for a company with greater than $5 billion of revenue, to 2.55% of revenue for a company with revenue less than $100 million. For smaller companies especially, these costs can be staggering.

In defense of SOX and the regulators who created it, costs related to compliance have been significantly declining. With the releases of the SEC's guidance for management with regard to SOX compliance and the Public Company Accounting Oversight Board's (PCAOB) release of Auditing Standard 5 (the replacement for the much-criticized AS2) in 2007, the costs of SOX compliance have continued to decline.

What is the lesson for private companies, nonprofit institutions, and other non-SEC registrants? The market has shown that public companies that reported material weaknesses in their internal controls over financial reporting did not experience a decline in their stock price. Or did they? Did a company that had a weak system of internal controls perform at its peak? Did the company take advantage of all of the resources available to it? Did the company create as much value as it could have for its stockholders and stakeholders? The overriding point is this: In the long run, companies and organizations that have a strong system of internal controls will prove to be winners in their respective marketplaces and industries. Strong internal controls help push a company beyond its current limits. Strong internal controls help a company implement best practices. Strong internal controls help a company ensure it is not wasting valuable resources. Strong internal controls help a company ensure it is serving its customers better than its competitors are.



Lessons from SOX

SOX was enacted as a response to several large-scale corporate scandals, including Enron, WorldCom, and Tyco. The legislation has been criticized as a knee-jerk reaction, implemented too quickly and without enough regard for its far-reaching implications. As mentioned above, the early implementers of SOX (larger public companies, "accelerated filers") incurred high costs and their finance and internal audit staff had to bear a heavy burden.

Interestingly enough, whereas almost 10% of companies reported material weaknesses in their systems of internal controls during the first year of SOX compliance, their stock price was hardly affected. In some cases, a company's stock price went up as the mar-

ket seemed to applaud those companies that were "strengthening" their internal controls. Conversely, financial restatements due to breakdowns in internal controls rose drastically, creating additional strain on organizations. As accelerated filers have continued to comply with SOX, there have been fewer financial restatements.

Why was SOX such a burden on organizations, both in terms of money and human resources? Because SOX was implemented in a time of panic for companies, auditors, and investors alike, its provisions were implemented in the extreme. Company managements and their external auditors were concerned about the ramifications of a poor system of internal controls, including huge shareholder settlements and potential jail time for company executives. In addition, the guidance published by the PCAOB (AS2) was read and interpreted as being extremely prescriptive in nature. Therefore, companies and their auditors took the provisions of SOX in their most literal sense.

All processes that had anything to do with financial statements were closely examined. All controls that mitigated even the smallest risks were documented and tested for effectiveness. Some companies identified and tested thousands of primary or "key" controls. Basically, a "bottom-up" approach was followed, meaning that processes and controls were identified, documented, and tested without much regard for the risks posed to the organization or its financial statements. The result was thousands of staff hours and millions of dollars. Not only did managements follow this approach, but so did their external auditors, causing audit fees to skyrocket.

Several executives of accelerated filers were interviewed and polled after their first year of SOX compliance. The results were overwhelmingly negative. The vast majority felt that the costs of SOX far outweighed the benefits. In fact, most questioned whether their organization gained any benefit from SOX.

After a few years and several lessons learned, a greater percentage of corporate executives are now starting to realize some of the benefits of implementing SOX. New guidance, notably the PCAOB's AS5, has been issued that has reduced some of the costs and greatly decreased the toll on companies' finance and internal audit staffs. Restatements are decreasing. The quality of relevant financial data is increasing, allowing company executives to make quicker, more nimble decisions. Several efficiencies, both in terms of financial reporting and operational excellence, have been gained. In addition, some companies are starting to use SOX as a springboard to a more holistic enterprise risk management initiative. Companies and their investors have started to realize the benefits of SOX and how it can strengthen a company.

Why Internal Controls Are Important for All Organizations

So why would a private company or a nonprofit organization want to endure the pain of SOX compliance described above if it is not required to? The bottom line is this: Strong internal controls provide a competitive advantage. Organizations with strong internal controls can respond more quickly to risk events and can turn risks into opportunities.

All organizations face risk. Risk can arise in many forms, including financial statement or reporting risk, fraud risk, reputational risk, environmental risk, and strategic risk. SOX was originally designed to address financial statement and reporting risk in addition to fraud risk. Why then, would an organization choose to address the risks surrounding reporting and fraud risk before other strategic, operational, or compliance risks? One compelling reason to start with financial and reporting risk is that it can provide immediate benefits. By implementing a strong system of internal controls over financial reporting, several short-term benefits can be realized, such as reduced incremental borrowing rates, increased confidence from investors or donors (in the case of a nonprofit), and a reduction in fraud exposure. In addition, from a succession planning standpoint, if a private company has a strong system of internal controls over financial reporting, the company is likely to yield more value in an acquisition and is better prepared to go public. Another reason is that there is an abundance of predefined tools, templates and methodologies that have already been developed for SOX compliance available from consulting firms, external auditors, and even on the Internet. These tools can typically be customized to fit any size or type of organization and can greatly reduce compliance costs. In addition, many consulting firms either have developed or are in the process of developing turnkey approaches to fit organizations of any size in several industries.

The risk of fraud in an organization, specifically the misappropriation of assets, should not be underestimated. The 2006 Association of Certified Fraud Examiners' Report to the Nation on Occupational Fraud & Abuse stated: "The median loss caused by the occupational frauds in this study was $159,000. Nearly one-quarter of the cases caused at least $1 million in losses and nine cases caused losses of $1 billion or more." The study also found that the median fraud scheme lasted only 18 months. Therefore, every year and a half, the typical company or organization will lose $159,000 due to fraud. It is thus very likely that if an organization were to halt only one fraud scheme with the implementation of a strong system of internal controls over financial reporting, the project would nearly, if not fully, pay for itself.

Implementing SOX and Best Practices

A large collection of best practices have already arisen from the implementation of SOX. Some basic best practices include performing a risk assessment, the identifying and documenting of internal controls over financial reporting, and continuously testing controls to ensure they are operating as expected.

Organizations that are not required to comply with SOX have much more leeway in constructing their systems of internal controls, as well as how they are documented and tested. Gone are the rigorous requirements of identifying all processes, risks, and controls that mitigate those risks. Gone is the need to test all controls to achieve a specific confidence interval that the controls are operating effectively. Gone is the need to satisfy stringent external auditor requirements. (Note, however, that Statements on Auditing Standards 104–111 significantly expand the way in which an external auditor is required to assess the risk of material misstatement.)

In private companies and nonprofits, the organization's management can be much more selective about the internal controls it chooses to identify or implement. That being said, management should consult with its external auditors on plans to implement internal controls over financial report-

ing. With the implementation of SASs 104–111 (commonly referred to as the risk assessment standards), external auditors will be placing more scrutiny on the internal controls of all organizations, whether public, private, or nonprofit. One of the objectives under the risk assessment standards is to require external auditors to gain a better understanding of the organization and its environment, including its internal controls over financial reporting, in order to identify the risks of material misstatement and what measures the organization is undertaking to mitigate those risks. Therefore, external auditors will likely start to place more scrutiny on internal controls. (Most have already.) One of the goals of external auditors with regard to the control environment is to help reduce substantive testing. It is important to consult with external auditors when preparing to document and test the control environment, as they may be able to partially rely on the work of management, which could help reduce external audit fees.

One of the most important best practices to come out of SOX documentation is the performance of a risk assessment. The purpose of a risk assessment is to identify the major risks facing an organization and to rank those risks in terms of likelihood and impact. Risk assessments can take many forms, from a plotted X-Y axis "heat map" to a tabular spreadsheet. The one thing all risk assessments have in common is that they give the user a visual definition of where the most important risks to the organization lie.

The content of a risk assessment varies depending upon the types of risks being assessed, be they strategic, operational, reporting, or compliance. When focused on financial reporting, a risk assessment is usually analyzed either by financial statement caption or by financial statement process (e.g., expenditure process, revenue process, treasury process). Each financial statement caption is then ranked using a variety of metrics, most commonly impact and likelihood. Impact is usually benchmarked using a materiality threshold. Likelihood is typically benchmarked using a combination of the centralization of the activity, complexity of the activity, the level of automation of the process, and the number of transactions the activity manages. By using a combination of these two metrics, inherent risk, or the risk of material misstatement before the application of internal controls, is derived. Based upon the level of inherent risk, management can decide where to focus its attention. No matter how the risks are ranked, risk assessments are only point-in-time documents. Therefore, they are only good as long as the original circumstances and assumptions the risk assessment was built around do not change. To remain effective, risk assessments should be updated at least annually.

Once the risk assessment is complete, an organization can begin to document the processes that pose the greatest risk to the entity. Documentation can take a multitude of forms, ranging from a process flowchart to a descriptive narrative, as long as it identifies the points within the process where "primary" or "key" controls take place. The definition of a key control is that it reduces the likelihood of a material error in the financial statements or reduces the risk of fraud (either fraudulent financial reporting or misappropriation of assets) to a remote possibility. While documenting key controls, it is important to note that these are the controls that will be tested for effectiveness. The easiest way to identify key controls is to begin by identifying the financial reporting or antifraud objectives that are contained within the process, then the primary risks to accomplishing those objectives, and lastly the key controls that sufficiently mitigate those risks.

As management is documenting its processes and corresponding control environment, it is very likely that there will be certain parts of the process that may not contain adequate controls to effectively reduce the risk of material misstatement or fraud to an acceptable level. These "design deficiencies" illuminate areas in which the organization will need to design and implement new internal controls to sufficiently address the risk.

The next step after the documentation of the control environment is to test the control environment. This is one area where the non-SEC registrant can be more efficient than the SEC registrant. Typically, external auditors require SEC registrants to test to a 90–95% confidence level, which may mean testing as many as 60 transactions (or more) or control instances for effectiveness. Non-SEC registrants don't typically need that level of rigor. In fact, the SEC's guidance for management no longer requires the management of SEC registrants to test to that level, but on a practical level, many external auditors will still likely test to a similar confidence level for high-risk areas. Other organizations can test enough to feel confident and comfortable that the control is operating effectively and as expected or designed. This will be different for all companies and could be different for each process or financial statement caption, depending upon perceived risk. In some cases, especially in a simple or centralized environment, the daily interaction and involvement by certain levels of management may be sufficient.

As management is testing its control environment, it will likely note areas in which controls are not functioning as designed or expected. These are called "operating deficiencies." The final step in testing the control environment is to remediate operating deficiencies. Operating deficiency control remediation can take many forms, including reengineering the process so as to further segregate duties between personnel or transfer the responsibility of the control to another operating unit. It may mean performing extra steps so that the control's performance is more apparent, and evidence can be collected. It may also mean abandoning the current control in favor of a more functional internal control or set of controls.

An Emerging Standard

A strong internal control environment is essential for all organizations, whether operating as a public entity, private entity, or nonprofit organization. SOX is slowly but surely evolving into a set of best practices, and something like SOX will likely become the standard, if not the requirement, for all companies in the near future. This trend is already clear in the most recently released risk assessment standards. Organizations that start these practices early will most definitely have a competitive edge over those that have not. They will be able to obtain the best financing, they will realize the best value in a merger or acquisition, and they will be able to take advantage of opportunities faster than their competitors. ❑

Chris Jeffrey, CPA, *is a senior manager in the risk services group at Virchow, Krause & Company, LLP, in Minneapolis, Minn.*