Top 5 SOX

WHILE most large and medium-sized companies have finished their first round of compliance, smaller businesses are still working on the provisions of Section 404 of the Sarbanes-Oxley Act of 2002 (SOX). I have been helping clients with SOX compliance since 2003, and, in working closely with management, I have found two challenging areas. The first is evaluating the design of internal controls, and the second is promoting the idea that, in general, the implementation of effective internal controls and/or processes could provide the company increased processing efficiencies and potential cost savings. Never mind SOX—how much time and money could a company save if management knew they could take proactive steps to implement key controls around significant processes? In 2004, how many companies had to test the same key controls multiple times before the operation of control appeared "effective?" How much more time and how many more resources did it take for the company to perform this undertaking?

In a survey about SOX compliance, internal auditors said that a company's three most common control issues were a lack of process control-related documentation,

Best Practices FOR SMALL COMPANIES

By Matthew A. Cozad, CMA, CFM, CIA

formal review and approval gaps, and not enough or proper segregation of duties. In light of these and other SOX compliance issues and concerns, five cost-saving opportunities have emerged that should enable smaller companies, who will be required to comply with SOX in 2006, to jump ahead of the learning curve and incorporate some valuable procedures and controls that will help them operate more efficiently and effectively.

1 Take Advantage of Checklists

The importance of a checklist expands beyond providing evidence about the performance of a key control; it clearly defines the scope of an employee's job responsibility and adds accountability. Realizing that clients struggle with showing they maintain clear audit trails for reviews, reconciliations, verifications, and other transactions, I have recommended that management use checklists to support employee accountability and to document the performance of key control activities. Moreover, I have seen smaller companies with less savvy IT operations come to appreciate the fact that paper checklists can reduce or eliminate their need to maintain volumes of paper to document reviews and approvals. Checklists also give management the ability to monitor whether recurring processes and tasks are completed on time. An example of a common checklist is a summary listing of all month-end journal entries that the preparer and reviewer initial and date to show evidence that the review and approval process was performed. The checklist is then included in the journal entry binder. The same type of checklist can be used for quarter-end financial statement preparation and review procedures, scheduled tax filings, etc.

In helping companies walk through and document significant processes, I have found that it becomes relatively easy to identify those controls that can be incorporated into monthly or quarterly checklists. In addition to the monthly or quarterly journal entries, some of the most useful checklists are for complex invoice reviews/reconciliations, budget-to-actual variance analyses, and quarterly/annual financial statement reporting processes.

2 Update Policies and Procedures

Existing policies and procedures serve as building blocks for SOX process documentation and define employees' roles and responsibilities. Once companies have identified significant SOX processes, documentation begins with evaluating those existing policies and procedures. The SOX documentation process is the most practical time to recommend ways to update any outdated or inadequate policies and procedures to avoid future pitfalls or control deficiencies.

One good example is recommending that management update their travel and reimbursement policy to account for changes in IRS regulations (*de minimis* thresholds). For instance, if company management and the internal auditors have identified employee expense reimbursements as a significant subprocess, then management is required to include the reimbursements within the scope of the company's accounts payable process. As part of the SOX documentation process, management and the auditors identify the staff accountant's review and verification of all documentation supporting an employee's expense reimbursement as a key control that's consistent with the company's reimbursement policy. As a result, the auditors' testing plans may include selecting a sample of employee reimbursements and verifying that they were properly authorized, accurately calculated, and supported by receipts to substantiate all reimbursable expenses.

Continuing with this example, say that as management and the auditors begin testing their sample reimbursement, they realize that the company's restrictive policy requires employees to turn in immaterial receipts for parking, gas, etc. As a result, those sampled reimbursements with any missing receipts would be considered testing exceptions. Even though those individual exceptions may be immaterial, a control gap would still exist, and management would need to go through the process of determining the significance of the gap using *A Framework for Evaluating Control Exceptions and Deficiencies*, which was published in December 2004 by BDO Seidman, Crowe Chizek and Co., Deloitte & Touche, Ernst & Young, Grant Thornton, Harbinger, KPMG, McGladrey & Pullen, and PricewaterhouseCoopers. Instead of performing the control gap evaluation process, management should update the company's travel policy to only require receipts for reimbursable expenses consistent with IRS regulations. That would add value to the company's operations as well as abide by the rules.

3 Implement a Disclosure Committee

Company procedures related to the disclosure of potential commitments and contingencies are receiving more attention as auditors attempt to evaluate and test the accuracy and completeness of financial statement disclosures. Such disclosures in a company's financial statements present challenges to management, in part because employees responsible for company transactions (e.g., leases, contracts, etc.) may not be aware of the need to communicate those arrangements to employees responsible for preparing the financial statement disclosures. In addition, those employees may be dispersed geographically or may not communicate regularly with employees outside their area.

Internal auditors and CFOs are taking a hard look at the processes and controls that companies have in place to capture items that require disclosure, such as operating leases, contracts, and agreements. One best practice I have observed companies implementing is the Disclosure Committee. A Disclosure Committee is composed of senior management from all areas of the organization, and its primary charge is to detect required financial reporting disclosure items. This committee also enhances the sharing of information across the organization and serves as a powerful entity-level control to communicate current and future business transactions, such as new contracts, acquisitions, reorganizations, and the like.

4 Ensure Adequate Segregation of Duties

As an organization progresses further through the documentation of significant processes, managers have more opportunities to quantify the importance of their role in the control environment. Management needs to clarify employees' roles and responsibilities, streamline or eliminate redundancies within processes, and achieve adequate segregation of duties over control processes.

I can't overemphasize the importance of adequate segregation of duties over the custody, approval, and processing of a company's transactions. I have come to appreciate the challenges smaller companies with limited resources face when inadequate segregation of duties is identified during the documentation phase of SOX. More often than not, I have seen that the roles of an employee performing a process and an employee responsible for reviewing the process for accuracy and completeness (the control) are often reversed (for example, a staff accountant reviews a senior manager's journal entries for accuracy). Another example of inadequate segregation of duties is when the employee responsible for completing a process (e.g., data input of employee salary information) is also responsible for verifying the completed task (e.g., review the payroll register for accuracy and completeness).

In situations where duties aren't segregated properly, management should cross-train employees to segregate incompatible duties and provide the opportunity for employees to assume more challenging roles and responsibilities to avoid this common pitfall.

The basic idea underlying segregation of duties is that no employee or group should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties. Principal incompatible duties to be segregated include:

- Custody of assets,
- Authorization or approval of related transactions affecting those assets,
- Recording or reporting of related transactions, and
- Execution of the transaction or transaction activity.

If an employee or group is performing duties in two or more of the above categories (e.g., the CFO signs company checks and records the disbursement in the company's accounting system), then management should evaluate the need to segregate those duties.

Giving employees this opportunity to cross-train or to assume more challenging duties may be a challenge for those managers who take ownership to get things done right the first time or who have a hard time delegating responsibilities as they advance in their careers. But adjusting, shifting, and redefining employees' roles and responsibilities are secondary to user access controls. From a practical perspective, conclusions regarding proper segregation of duties can be adequately tested only through an evaluation of physical and application user access.

Regarding technology, a company's internal auditors evaluate the segregation of duties via up-front reviews of user access to significant financial applications to assess potential risks. When I have conducted such reviews, more often than not I've found that members of management who have authorization access to the company's assets also have the same user access as those employees who are responsible for recording journal entries and reconciling the general ledger. I've also found that managers who have authorization to approve transactions feel the need to keep the same access levels as their subordinates to perform more complicated entries or to correct errors during the financial statement closing process. This is unacceptable in today's IT environment, and, if it isn't changed, is a sure path to significant or even material weaknesses. To remedy this potential control weakness, the application system administrator should provide read-only access to management responsible for authorizing transactions and/or reviewing the accuracy and completeness of completed transactions (e.g., journal entries, bank and general ledger reconciliations, etc.).

In companies that have a variety of user access groups (e.g., query only, administrator, or general ledger user) or who have frequent turnover or reorganizations, management should perform a detailed quarterly or semiannual review of user access to incorporate into the company's existing controls. In addition, more technology savvy auditors are recommending to management the value of using computer-assisted audit techniques (CAATs), such as data extraction software, as a means to effectively evaluate user access, segregation of duties over journal entries, and other security issues.

5 Don't Forget SAS 70 User Control Considerations

User-access reviews, segregation of duties, checklists, policies and procedures, and entity-level controls remain internal to an organization. What happens when a company outsources functions or relies on an outside vendor to provide core and/or support services that management relies on to support the assertion that the financial statements are fairly presented in accordance with GAAP?

As required by SOX, management should consider the activities of any service organization it uses when assessing its own internal controls over financial reporting. These rules are covered in Statement on Auditing Standards (SAS) No. 70, "Reports on the Processing of Transactions by Service Organizations," which spells out how an external auditor should assess the internal controls of the service provider used by the company it is auditing. Current SOX guidance recognizes that obtaining an SAS 70 Type II report from the service provider constitutes acceptable documentation and will allow a company to properly evaluate the operating effectiveness of controls at the service organization. (A Type II report includes, among other things, the external auditor's opinion on the fairness of the presentation of the service provider's description of its controls and how well suited the controls are to achieve the specified control objectives as well as the auditor's opinion on whether the controls were operating effectively during the period under review.) Based on my experience with SAS 70 control evaluations, the most difficult part of management's assessment includes an evaluation of recommended "user control considerations." User control considerations are recommended by the service provider for companies to have in place to support the achievement of the service provider's control objectives.

Common examples of controls that service providers recommend include:

- Review of service provider reports provided to the company for accuracy and completeness.
- Controls over granting user access to the service provider's systems.
- Establishment of authorization limits within a company.
- Maintain adequate segregation of duties, and ensure that employees' roles and responsibilities are clearly defined.
- Controls over backup and recovery of data received from the service provider.

Companies document their evaluation of user control considerations through matching existing company controls to the service provider's recommended controls. If there's a gap, management should evaluate the significance of the recommended control and potential mitigating controls within the company. To support the performance of the evaluation, I recommend that management present the results of the SAS 70 review to the Disclosure Committee or senior management.

If a service provider doesn't have an SAS 70 Type II report, management needs to clearly identify the provider's services that it relies on and ensure that adequate controls are in place internally to detect errors, omissions, etc. In most situations, it isn't realistic for management to inspect and test the service provider's internal controls. Under the Public Company Accounting Oversight Board's (PCAOB) current guidance, this may present a company the opportunity to extend a contract to another service provider that does offer a Type II report. Regardless, members of management who are most familiar with the provider's services need to work closely with the auditor to ensure that adequate attention is given to support management's overall SAS 70 review.

Take the Opportunity

Instead of viewing SOX as merely one of the many compliance hurdles they face today, small business managers/owners need to think of it as an opportunity to improve corporate governance, policies, and procedures and to reduce corporate costs. From an auditor's viewpoint, I believe a tremendous opportunity has emerged to incorporate the results from SOX testing (identified deficiencies and best practices) into future risk assessments, scoping of internal audits, reengineering, and other processes.

Whether it's in the implementation of revised policies and procedures, the use of CAATs, or the creation of checklists, SOX has refined management's focus on those financial-related processes that require continuous benchmarking and evaluation. Moving forward, companies will need to perform regular evaluations of their internal controls over financial reporting. I would be the first to agree that it's hard to sell management on the idea of implementing controls or best practices when there are no errors, omissions, or other material misstatements that require change. Yet, "where there is smoke, there is fire," and I think that auditors, having learned from their 2004 SOX experiences, are in a better position to recommend change earlier so management can prevent some of the costly mistakes the first compliers made and be able to run their businesses more efficiently and effectively. ■

Matthew A. Cozad, CMA, CFM, CIA, is a supervisor with Keiter, Stephens, Hurst, Gary & Shreaves in Glen Allen, Va. He provides risk management services to clients that outsource the internal audit function and assistance to companies planning, documenting, and testing key internal processes subject to SOX compliance. You can reach Matt at (804) 565-6007 or mcozad@kshgs.com.