SOX 404: How Do You Control Your Internal Control?

J. Ralph Byington and Jo Ann Christensen

Section 404 of the Sarbanes-Oxley Act (SOX) makes most publicly traded companies report on the effectiveness of their internal controls. That can be a daunting task. But this article offers practical advice and valuable checklists that will make the job easier. © 2005 Wiley Periodicals, Inc.

What has happened to the business world in the wake of the accounting and auditing scandals of companies such as Enron, WorldCom, and Healthcare? In the corporate environment following these scandals, upper management and the accounting profession, not to mention the public and the press, found themselves pondering how these scandals could have occurred and what should be done to prevent them from recurring in the future. As they were *pondering,* the federal government enacted the Sarbanes-Oxley Act (SOX) of 2002 and came *banging* on the corporate doors of most publicly traded firms.

The objective of SOX was to make company audit committees, the auditing profession, and corporate management work together to reduce the risk of these types of scandals recurring (McDonnell, 2004). Section 404 of SOX requires the majority of publicly traded companies to include a report on the effectiveness of their internal controls. This report must be: (1) included in the company annual report, (2) certified as to its accuracy by upper management, and (3) attested to by an independent audit firm. Components of the report must include: (1) a statement describing management's specific responsibility for the establishment and maintenance of an adequate internal control system, (2) the description of the framework to evaluate the internal controls, (3) a statement of the effectiveness of the internal control system at year-end, and (4) a statement that indicates that the independent auditors have issued a report attesting to management's assessment of the company's internal controls (Ramos, 2004a, 2004b). The purpose of this article is to present some suggestions and checklists that will help both the company management and the independent auditor to be in compliance with Section 404 of the Sarbanes-Oxley Act.

INTERNAL CONTROL

The Foreign Corrupt Practices Act (FCPA) of 1977 requires publicly traded companies to establish a system of internal accounting controls. The purpose of these controls is to protect company assets from theft and loss and to provide assurance as to the reliability and material accuracy of the company's financial statements. Internal controls can be divided into administrative controls and accounting controls. Administrative controls include the organization plan and the procedures and records involved in decision processes that lead to the authorization of transactions. Accounting controls include the organization plan and the procedures and records involved in safeguarding assets and the issuance of reliable financial records (Robertson & Davis, 1982). Following are some suggestions and checklists that should help management and

Published online in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/jcaf.20116

the independent auditor assess the reliability of both administrative controls and accounting controls.

MANAGEMENT CONSIDERATIONS

It is the responsibility of management to establish, operate, maintain, and improve internal controls. To begin this process, management should be familiar with the characteristics of a reliable internal control system. See Exhibit 1 for a list of these characteristics.

Section 404 specifies that management must identify, document, and evaluate significant internal controls (Ramos, 2004a). During the process, special attention should be given to the control environment. This attention is warranted because the control environment is a key component of a company's internal control. It is a key component because: (1) it will set the tone of the company, (2) it will influence the control consciousness of the individuals within the company, and (3) it is the basis for all other aspects of internal control (Ramos, 2004a). It is important to note that management cannot delegate any of these responsibilities (McConnell & Banks, 2003). See Exhibit 2 for a checklist of action that management can employ to ensure compliance with SOX.

INDEPENDENT AUDITOR CONSIDERATIONS

As noted above, SOX requires the independent audit firm to audit management's assertions regarding the effectiveness of internal controls. The independent auditors must perform their own tests of controls and not rely on management's tests. Under SOX, the primary focus of the tests performed by the independent auditor concerns the reliability of the internal controls (Ramos, 2004a). At a minimum, the independent auditor should: (1) have an understanding of the control design, (2) evaluate the effectiveness of the control design to determine if it is designed in a manner to detect or prevent material misstatements in a timely fashion, (3) evaluate and test how the control was applied, whether it was applied on a consistent basis, and who was responsible for applying it, and (4) form an opinion on how effective the system of controls is. Additionally, special attention should be given to the control environment (McConnell & Banks, 2003). This attention is warranted for the same reasons specified above for management (Ramos, 2004a). See Exhibit 3 for a checklist of tests that should be useful to the independent auditor in order to be in compliance with SOX.

AREAS OF SPECIFIC CONSIDERATION

The suggestions and checklists above are fairly general in nature, and management and the independent auditor will have to make judgment calls as to what elements are relevant to them and their needs. However, there are some specific areas that all parties involved in the compliance process should pay close attention to. These areas include

Exhibit 1

Characteristics of a Reliable Internal Control System

1. Personnel should possess qualities commensurate with their responsibilities.
2. There should be an organization plan that specifies appropriate segregation of functional responsibilities.
3. There should be a system of authorization, objectives, techniques, and supervision that provides accounting control over revenue, expenses, assets, and liabilities.
4. There should be control over access to assets, important documents, and blank forms.
5. There should be a periodic comparison between records and actual assets and liabilities and action taken to correct any differences.

(Robertson & Davis, 1982)

Exhibit 2

Chief Financial Officer and Controller Checklist

1. Confirm that accounting practices, policies, and procedures are in accordance with generally accepted accounting principles. Compare the accounting policies with industry accounting policies.
2. If not already addressed, consider drafting policies and procedures for the following areas:
   a. Financial statement accuracy
   b. The relationships and expectation concerning working with internal auditors
   c. The relationships and expectations concerning working with independent auditors
   d. Loans to executive officers and directors
   e. Off-balance sheet transactions
   f. Pro forma financial statement information
   g. Insider and related party transactions
   h. Assessment of control systems
   i. Code of ethics
   j. Treasury procedures and risks
3. Communicate your accounting practices, policies, and procedures so that they are understood by all affected staff.
4. Provide needed training in accounting practices and policies to enable the individuals held responsible for the following tasks to perform them correctly and completely:
   a. Recording of transactions
   b. Developing information to be used to formulate and record expense and loss provisions
   c. Preparing financial statement disclosures
5. If there are multiple sites where the accounting transactions and the financial disclosures are compiled and processed, ensure that the foregoing practices, procedures, and training deal with the unique environment at each site.
6. Confirm compliance with accounting practices, policies, and procedures.
7. Confirm that accounting and financial practices and procedures are addressed in the Code of Ethics. Include operating and financial managers, when appropriate, in the certification process.
8. Make certain the guidelines for developing and recording estimates are documented and understood.
9. Establish procedures to documenting, analyzing, and reconciling balance sheet accounts/off-balance sheet accounts to ensure that these activities occur as scheduled. Verify that a process exists for resolving issues or presenting unresolved differences to upper management in a timely manner.
10. Establish a process/system that allows disclosures of material changes in the financial condition or results of operations within two business days after the fact or event causing the change. Make certain the company Web site allows for disclosure requirements.
11. Evaluate the speed of production of operational and financial information required to make informed decisions. Make the changes required to hasten its accessibility.
12. Reconsider the correctness of existing key performance indicators for the company and expand them when necessary.
13. Attend to and implement all audit recommendations, especially those that concern weaknesses in internal controls.
14. Implement a process to make certain that press releases are verified in terms of missing or misleading information before issuance.

(continued)

Exhibit 2

Chief Financial Officer and Controller Checklist *(continued)*

15. Implement/formalize a process to make certain that information offered in Management's Discussion and Analysis is the same as the information in the financial statements and footnote disclosures.
16. Educate senior officers (e.g., HR, legal, operations) about whistleblower and retaliation provisions of SOX. Document retention practices and appropriate corporate practices.
17. Make certain that the departments that oversee 401(k) and pension plans have procedures that prohibit trading in the company securities for the duration of any blackout periods. Work with employees to instruct them on the process for notification of blackout periods.
18. Educate directors and officers regarding activities that are prohibited by the SEC.
19. Bar hiring any individual(s) previously employed by the independent audit firm that was involved in an audit during the last 12 months as the chief executive officer, chief financial officer, or controller.
20. Authenticate and document risks facing the business.
21. Make certain that purchases of all finance and related services are from approved no-conflict suppliers.

(Parson Consulting, n.d.)

the use of spreadsheets, outsourcing, and computer security.

Spreadsheets are frequently used by accountants to organize and summarize accounting data, and management will have to certify the accuracy of this information. By nature, spreadsheets will vary according to usage and complexity and the control requirements may vary from one spreadsheet to the next ("Section 404 Compliance," 2004). PricewaterhouseCoopers (PwC) has developed a five-step program for evaluating spreadsheet controls. See Exhibit 4 for the major points of PwC's program.

The use of financial process outsourcers, known as service organizations, adds another complication to compliance with Section 404 of SOX. To date, the professional standards fail to clearly specify the responsibilities of management, the service organization, and the independent auditor under SOX. However, if the service organization initiates transactions, rather than simply executing transactions authorized by the client company, then there can be a significant impact on the level of internal control evaluation by the client company and the independent auditor. Thus, it would seem that if the service company doesn't initiate any transactions, the client company and the independent auditor may only have to give secondary considerations to the service company's internal controls. It would, however, be necessary for the management of the client company to have put in place internal controls regarding dealing with the service company. In general, it is incumbent upon the client company and the independent auditor to consider the service organization's internal controls (Harris, 2004).

Under SOX, computer security becomes a very real concern. Specifically, access to systems, the security of systems, and systems change become areas that need to come under scrutiny when management and the independent auditor are endeavoring to be in compliance. The professional standards state that there will be strict monitoring of the independent audit firm's approach to evaluating, examining, and reporting on the technological aspects of the company's financial reporting process. Furthermore, all parties involved in the SOX compliance process find themselves in a position where they must have an understanding of data that goes through the system. Both management and the independent auditor must seek assurance that the data from the system emerges accurately and securely (Krell, 2004). A discussion of the detailed procedures and controls necessary to achieve this understanding is too lengthy for this article. However, it should be clear that any computer system or program should be password-protected.

Exhibit 3

Key Proposed Tests of Controls

1. An effectual detective control can make up for a deficient preventative control, thus preventing a significant deficiency or material weakness.
2. The auditor should extensively test controls upon which other significant controls rely.
3. Evidence regarding the control environment, including fraud programs, frequently is highly subjective; the independent auditor should not rely upon results of tests others perform.
4. The independent auditor should restrict use of work done by others in areas such as controls over major nonroutine and nonsystematic transactions and the end-of-period financial reporting process.
5. The independent auditor can test controls at an interim date, unless the control environment is deficient. Consideration should be given to getting additional evidence for the remaining time period.
6. When the entity has changed controls, the independent auditor does not need to ordinarily consider the superseded controls to express an opinion on controls that are effective at year-end; however, the controls that have been changed could relate to reliance on controls during the financial statement audit because of the nature of earnings and cash flow measurement.
7. If the reasons for a control exception don't indicate a weakness in basic design or control operation, the difference may not indicate a major deficiency.
8. Whatever the reasons, numerous or repeated occurrences of a deficiency may represent a major deficiency.
9. Even though individually insignificant, several control deficiencies with a common attribute or feature could represent a major deficiency.
10. A material misstatement that the independent auditor detects but the company does not identify usually is a material weakness in controls.
11. Where numerous locations exist, the independent auditor should perform tests of controls when a location is:
    a. Individually important
    b. Individually not important, but presents definite risks that might be material to the financial statements
    c. Individually not important, but could be when aggregated with other locations

(McConnell & Banks, 2003)

CONTROLLING INTERNAL CONTROLS

We have noted that as early as 1977, government regulations required publicly traded companies to establish a system of internal accounting controls. In the wake of the accounting and auditing scandals of companies such as Enron, WorldCom, and Healthcare, it became obvious that while required to have a system of internal control, not all companies had effective internal controls. As a result, the government stepped in again and enacted the Sarbanes-Oxley Act of 2002. Beginning in 2004, many corporations must comply with Section 404 of SOX. This section requires the majority of publicly traded companies to include a report on the effectiveness of their internal controls. This report must be included in the annual report, certified as to its accuracy by upper management, and attested to by an independent audit firm. The penalties for not accurately certifying the system of internal control can include fines and/or prison sentences.

In this article, we have provided corporate management and the independent auditor with some practical suggestions and valuable checklists that will assist them in their efforts to be in compliance with SOX. Will future scandals bring even more stringent requirements? Companies should keep a close eye on

Exhibit 4

Five-Step Program for Evaluating Spreadsheet Controls

Step 1. Inventory the spreadsheets. For each spreadsheet, include:
- a. Spreadsheet name
- b. Description of spreadsheet, including calculated financial statement amounts
- c. Department responsible for spreadsheet development
- d. Departments that use the spreadsheet
- e. Frequency and extent to which the spreadsheet is changed

Step 2. Evaluate spreadsheet use and complexity.
- a. Uses include operational, analytical, and financial
- b. Complexity includes low, moderate, and high

Step 3. Ascertain the controls needed for each statement. Controls will need to either:
- a. Protect the spreadsheet data or
- b. Ensure physical security of the spreadsheet.

Step 4. Evaluate each spreadsheet's existing controls. Compare existing controls against the checklist of necessary controls.

Step 5. Develop a remediation plan for control deficiencies

("Section 404 Compliance," 2004)

the situation in the coming years.

REFERENCES

Harris, R. (2004). Facing challenges: Outsourcing financial processes in the era of Sarbanes-Oxley. AFP Exchange, 24(6), 32–35.

Krell, E. (2004). Foolproof compliance for your IT systems. Business Finance, 10(11), 46.

McConnell, D. K., Jr., & Banks, G. Y. (2003). How Sarbanes-Oxley will change the audit process. Journal of Accountancy, 196(3), 49–55.

McDonnell, P. J. (2004). The PCAOB and the future of oversight. Journal of Accountancy, 198(6), 98–101.

Parson Consulting (n.d.). Chief financial officer and controller checklist. Retrieved January 11, 2005, from http://www.parsonconsulting.com/sarbanes-cfo_control.asp

Ramos, M. (2004a). Evaluate the control environment. Journal of Accountancy, 197(5), 75–78.

Ramos, M. (2004b). Section 404 compliance in the annual report. Journal of Accountancy, 198(4), 43–48.

Robertson, J. C., & Davis, F. G. (1982). Auditing (3rd ed.). Plano, TX: Business Publications, Inc.

Section 404 compliance: Five-step PwC program ensures mgrs can certify spreadsheet data. (2004, December). The Controller's Report, pp. 1–4.

J. Ralph Byington, PhD, CPA, is the Timmerman Chair in Enterprise Development and a professor of accounting at the University of South Carolina–Aiken. His publications include over 100 journal articles, book chapters, newsletter items, and proceedings. He is active within the accounting profession, presenting numerous professional programs at the national, regional, and local levels. He has presented over 250 professional programs to business executives, CEOs, CFOs, state CPA societies, student organizations, and firms in Georgia, Louisiana, Mississippi, Texas, New York, California, Illinois, Massachusetts, Florida, Arkansas, and Washington, D.C. **Jo Ann Christensen,** DBA, is an assistant professor in the School of Professional Accountancy at Louisiana Tech University. She is published in the accounting area with expertise in protection against white-collar crime and ethical behavior in company reporting.