November 2004

Sarbanes-Oxley Section 404 White Paper

Complying with the Provisions of the new Law: Documentation and Controls Attestation

Author: *Lynda Radke, CPA*
CFO, ProCognis, Inc.
info@procognis.com

Abstract

The following discussion provides a brief overview to prepare financial professionals with a basic background on complying with the Sarbanes-Oxley act Section 404. Topics include preparation and planning prior to implementation, documentation and testing of control structures.

1. The Law

On May 27, 2003, the Securities and Exchange Commission ("SEC") adopted the rules related to «Management's report on internal control over financial reporting and certification of disclosure in exchange act periodic reports.» These rules were adopted to comply with the requirements of Section 404 of the Sarbanes-Oxley Act of 2002. The final rules require that each annual report contain: (1) a statement of management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and (2) management's assessment, as of the end of the company's most recent fiscal year, of the effectiveness of the company's internal control structure and procedures for financial reporting. This section also requires that the company's outside auditors attest to the report on management's assessment.[i] This means that companies should self-evaluate well before their compliance date.

2. Transition and Timing

Accelerated filers, generally those companies with market capitalizations over $75 million, and who have previously filed an annual report with the commission, are required to comply for fiscal years ending on or after November 15, 2004. All other issuers are required to comply for fiscal years ending after July 15, 2006.[ii] Because of the amount of time expected to be needed in order to implement these provisions it is recommended that all companies begin the implementation process *as soon as possible*.

Note

Accelerated Filers must comply before their 2004 fiscal year end. Other filers must comply before their 2006 fiscal year end.

3. Basic Requirements

While the rules require that management assess the effectiveness of the company's internal control structure, the rules do not specify a framework for making such an assessment. What they do specify is that the framework "be a suitable, recognized, control framework that is established by a body or group that has followed due-process procedures, including distribution of the framework for public comment." By far the most widely recognized framework, that meets this definition is the framework designed by the Committee of Sponsoring Organizations of the Treadway Commission. This framework was published in 1992 and is known as the COSO framework.[iii]

The final rules do not specify a level of testing or documentation, nor do they specify the treatment of identified weaknesses. As a result of the lack of specificity in the final report, a variety of different approaches have been taken by those implementing the new rules. What follows represents our opinions on how to comply with Section 404 using the COSO framework. As each company is unique there is no substitute for professional judgment. We also believe in the importance of having competent advisors and conferring with them as necessary.

4. Planning

The first step in achieving compliance is a plan of action. We strongly believe in having a written plan which should be communicated with the company's Board, Management, and Audit Committee. In addition, obtaining feedback from the company's advisors and outside auditors can help ensure that everyone is in agreement on what is to be done, and prevent additional work at the last minute.

- *Staffing*
  The plan should include information relating to who will be doing the work. Will there be a project leader? Will there be employee(s) dedicated to the project? How will employees balance their other workloads? When will the work take place? Will the company utilize consultants or "outsource" the work? Independence rules prohibit the company from relying on its external auditors to perform the evaluation, as it would result in the auditors attesting to their own work. The rules, however, allow the auditors to assist management in other ways, such as providing templates or helping to document controls, as long as management makes all final decisions an exercises its own judgment.
- *Framework*
  The plan must also include whether the company will be using the COSO framework or another framework. In the management assessment you will be required to disclose which framework you use. Care should be taken to make sure that the framework chosen meets the requirements of the final rule.
- *Systems Identification*
  In the planning process, key systems should be identified and agreed upon by all parties. Systems can be broad (such as the disbursements cycle) or more narrow (such as purchasing) depending on the structure of the organization. The company will also need to determine if you will be evaluating systems on a company-wide basis or on a more decentralized basis. The answer may be different for different systems. For example, a company may have a centralized purchasing department, but then has an accounts payable department for each subsidiary. In that case it would make sense to

treat the purchasing department as one system and then treat each separate accounts payable department as a separate system. Even if all the accounts payable departments have the same procedures, the effectiveness of those procedures could differ from department to department. Splitting them into separate systems would allow the company to identify just those areas where controls were not effective. Reporting lines can be a useful tool in determining how to separate systems. Some examples of common systems include: purchasing/accounts payable/cash disbursements, sales/accounts receivable/cash receipts, treasury/cash management/investing, inventory, month end closing, quarter end closing, fixed assets, tax reporting, financial reporting. The important thing to remember is that no two companies are the same, and the systems you report must make sense for the organization.

- *Control Environment*
  All companies operate within a certain control environment. Internal and external forces exert pressures on that environment. It is important that the company accurately assess its control environment. What pressures do management and staff face? Will these pressures make them more or less likely to become a party to fraud? What about the detection of fraud? Perhaps staff has no motivation to commit fraud, but is so overworked that key oversight activity simply doesn't happen. What about employee turnover? What subtle clues do management, and the board of directors, give employees about their tolerance of fraud? All of these issues, and many others, contribute to the control environment within a company. It is important to note that an assessment that a company has a high risk control environment doesn't necessarily indicate the presence of fraud. What it tells us is that there is inherently more incentive to commit fraud within that company. All things being equal, a company with a high risk control environment will need a tighter internal controls structure and more oversight then a company with a lower risk control environment.

- *Testing Level*
  After assessing the control environment, it is advisable for a company to set some parameters for testing levels. This will ensure that work performed by different team members is consistent. It is also advisable to seek feedback from the company's outside auditors to make sure that they concur with the proposed testing level.

5. Document Systems and Steps

After the planning phase has been completed, the next step is to begin documenting the systems identified. This process may involve meeting with and interviewing the employees directly responsible for performing the tasks, as well as the manager responsible for that department or area. Understand and document how a system works from the triggering event to the completion event. If the system is accounts payable, the steps might include, receiving the invoice (triggering event), coding the invoice to a general ledger account, inputting the invoice into the AP system, obtaining approval of the invoice, printing a check, matching the check to backup, obtaining a signature, obtaining a second signature, mailing the check, recording the payment, relieving accounts payable, and reconciling the bank account (concluding event). Once again, every company is different and the steps you document should reflect the activity at your company. In this process it is possible that you will uncover additional systems, or find out more information about the previously identified systems that may change the original plan or assessment.

6. Identify and Evaluate Risks

Once the systems and steps are documented, consider what could go wrong at each step of the process. Multiple risks may be identified for certain steps. Other steps may have no risks. These risks should then be evaluated to determine which pose the largest threat to the accuracy of the company's financial reporting system. The evaluation should be based on the underlying risk, assuming that no controls exist.

7. Document Mitigating Controls

As you are documenting risks, you are probably thinking to yourself, "that could never happen because…" or "that would be detected by…" Both of these are examples of mitigating controls. Some controls prevent an act from taking place, others expose the act shortly after it has happened, thus deterring a perpetrator. For each identified risk, an appropriate control should exist. As controls are identified, consider if the design of the control is sufficient to mitigate the risk. This process will most likely result in the identification of one or more unmitigated risks. The final rules prohibit management from concluding that the company's 'controls over financial reporting' are effective if there is a material weakness in internal controls.[iv] As a result, it is necessary to determine if this control deficiency rises to the level of a material weakness, as that term is currently used in accounting literature. If time permits, a control should be designed to mitigate this risk regardless of the assessment of it.

8. Test the Effectiveness of the Controls

This is the heart of your 404 compliance - where most of the time will be spent. Not only must the design of the control be sufficient to mitigate the risk, but the operating effectiveness of the control must be evaluated. In addition, the company must maintain evidential matter to provide reasonable support for management's conclusion regarding the effectiveness of the internal controls. This means the company will need to test the controls and maintain documentation of the testing work performed. While this might not sound like much on the face of it, when you consider the number systems that have been identified, each with multiple steps, which may in turn have multiple risks, each of which may in turn have multiple controls, it is easy to see how this can become a very time-consuming process. And, what's more, this testing and controls evaluation will be required each year from now until the foreseeable future.

Note

Your Auditors *may not* accept control testing on transactions which occurred prior to the current fiscal year. Testing must take place in the year of Section 404 implementation. For example, for Dec. 31, 2005 implementation, no 2004 transactions can be used to document compliance.

As we have previously said, the final rules do not specify the level of testing or documentation. However, your outside auditors will be attesting to your assertion about the effectiveness of the company's controls. They will determine if management has performed sufficient testing to evaluate the controls, and if management's conclusion about those controls is appropriate. Frequent and early communication with your outside auditors can prevent misunderstandings and allow time to rectify any perceived weaknesses.

9. Evaluate Test Results

As each test is completed, evaluate the results. Was the design of the control significant to mitigate the risk? Did the testing provide evidence that the control is operating effectively? Does the company have sufficient documentation to support its assertions?

10. Modify Controls

If in the evaluation process, one of the identified risks is not mitigated, controls will need to be modified or new controls created. Controls may have been in place that weren't being followed. Company staff may require additional training before a control can be considered effective. Policies and procedures will need to be established and enforced.

11. Remediation

Once the new controls have been put in place, some time must pass before it makes sense to evaluate these new controls. The earlier the company begins the project the more time their will be for this process. Throughout the process documentation should be kept showing the original testing, what the remediation process was, and the results of the retest.

12. Auditor Attestation

The external auditors are required to attest to management's assertion regarding internal controls. To do so, the auditing firm must perform enough work to assure itself that management has designed and implemented appropriate controls and that management has performed a sufficient level of testing to evaluate the effectiveness of those controls. Scheduling is key here, especially if you have a calendar year-end. If you schedule the work to be performed too close to year-end, and an issue arises, you will have little time to correct the situation. If you schedule too early, you may not be able to complete the work on time. It would not be surprising if the audit firms see many of their audit clients requesting this work be performed 2 to 3 months prior to their year end. If all goes well, in the company's annual report, management makes the assertion that their internal controls are effective, and the external auditor's attest to that assertion.

Note

Financial statements are now required to include an attestation of control effectiveness. This attestation reflects both design and operating effectiveness (i.e. tested and proven effective). Any control breakdowns, whether found to be ineffective in design or in practice may require you to disclose material weakness in your controls.

13. Next Steps

While very expensive products exist to aid in the initial documentation and description of the existing controls, what's really needed is a solution to aid in producing ongoing testing and evaluation. We feel the best solution is a documentation framework and a set of reusable templates that capture your system and controls design and provide a common repository to simplify testing and collect all relevant data.

While a large investment is required for complex companies in initial compliance, the vast majority of companies will not require the group of current product offerings that focus on a narrow aspect of compliance. We provide a cost-effective product that meets the current needs of small and mid-sized companies for documentation but also meets the needs for ongoing testing and evaluation for all companies. We call this product «Sarbanes-Oxley 404 Compliance Tool» and provide this product for under $4,000. While it does not relieve you of all tasks, it does greatly simplify the task and codifies best practices for compliance, in our view.

Conclusion

Despite the tremendous effort that most companies will put into their initial 404 compliance, the requirements don't stop there as companies are required to make the same assertion every year. For future years, there will be more focus on new systems and changes to existing systems. Acquisitions of privately traded companies may require a substantial amount of work to bring them into compliance. Even acquisitions of publicly traded companies will require system documentation and new testing. To minimize ongoing cost, companies will want to streamline their systems as much as possible. It is also a good idea to have a system in place that allows a company to leverage the previous years' work. While large diversified companies may need a sophisticated system, most companies can benefit from an easy to use template-based system.

About the Author

Lynda Radke has a degree in Business Economics with an emphasis in Accounting from the University of California Santa Barbara. She began her career with Deloitte & Touche and entered the private sector and quickly rose as the CFO of a publicly traded Bank holding company. There she spearhead FDICIA compliance and had extensive experience with the COSO framework. Currently she is the co-founder of ProCognis, Inc., a software and professional services company that specializes in financial reporting and other SEC matters. ProCognis Inc. is the developer of the SOX 404 Compliance Tool used to assist companies to document and test their internal controls in compliance with Sarbanes-Oxley.

[i] Speech by SEC staff: The SEC's Internal Control Report Rules and Thoughts on the Sarbanes-Oxley Act
[ii] 2003-66: SEC Implements Internal Control Provisions of Sarbanes-Oxley Act; updated to reflect revised deadlines.

[iii] Speech by SEC staff: The SEC's Internal Control Report Rules and Thoughts on the Sarbanes-Oxley Act

[iv] Speech by SEC staff: The SEC's Internal Control Report Rules and Thoughts on the Sarbanes-Oxley Act

Disclaimer

While the proceeding information reflects our best interpretation of the prevailing law and industry best practices, implementation of this or any other financial function must involve careful consultation with your SEC counsel and audit firm. Furthermore, the above discussion cannot encompass all details for each company or organization and professional judgment will dictate the proper course of action in your particular case.