January 2005

Sarbanes-Oxley Section 404 Planning and Documentation

Complying with the Provisions of the new Law: Developing a Compliance Plan and Documenting Controls

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

Abstract

This Whitepaper is intended for those already familiar with the basic provisions of Sarbanes-Oxley Act, Section 404. If you are not yet familiar with the Act, we suggest you read our overview whitepaper 'Sarbanes-Oxley Section 404 White Paper: Complying with the Provisions of the new Law.'

Compliance with the Sarbanes-Oxley Act can be broken into four stages: Planning, Documentation, Testing and Evaluation. This whitepaper provides more in-depth guidance regarding implementing the Act: specifically the Planning and Documentation requirements.

1. Planning for Sarbanes-Oxley 404 Compliance

Planning is an extremely important part of your compliance process. Not only will it help you plan out the path ahead, but it becomes a valuable starting place for discussing the project with your auditors and audit committee. The planning process is a valuable time to form consensus, formalize the compliance plan and define responsibilities. Any differences of opinion should be resolved at this stage and not after you have expended time and effort.

We recommend a formal written plan which encompasses, at minimum, the following areas:

- **Staffing:** Define who is responsible for an area of compliance and plan feedback and communication with members of the team, audit committee and external auditors.
- **Timing:** Divide the task into key deliverables and plan a schedule for implementation.
- **Framework selection:** Select a recognized framework (such as COSO) [1] to construct your testing plans and ongoing compliance tasks.
- **Selection of major systems or cycles:** Define business systems (e.g. Sales, Accounts Receivable, Cash Receipts, Inventory, etc.) and correlate each system to components of the financial statements.
- **Control environment assessment**: Examine risk-tolerance and anticipated impact for a control failure on a company-wide level.
- **Test planning**. Define the testing level (e.g. number of selections, rotation plan, handling test failures, etc.) and define a consistent testing methodology. [2]

> ***Note***
> Section 404 requires selection of a "recognized framework" and a consistent testing methodology.

2. Staffing Considerations

In the planning process, take some time to consider how you will staff this project. In order to successfully complete this project you will need both knowledge and capacity. There are four basic ways that you can staff this project:

1. *Complete Outsource*
   This is the most expensive option. The use of consultants or outside services doesn't allow for a transfer of the compliance expertise to in-house staff and may leave you vulnerable if the consulting or services firm goes out of business, experiences significant turnover or raises their rates unexpectedly. The consultants may also have difficulty obtaining information from your staff without in-house guidance and help answering their questions. However, this option may make sense if your business requires your entire staff to focus on other priorities. A significant merger, major new product release or the implementation of a new GL system might be so taxing on your staff that you simply have no remaining resources to devote to compliance. You might consider this if you were lacking knowledge or if you were lacking knowledge and capacity.
2. *Co-Source*
   Co-sourcing the project allows your staff to work together with consultants to reach compliance. Co-sourcing works great for companies that have some in-house staffing capacity but lack knowledge in the compliance process. Co-sourcing also allows you to work towards self-sufficiency by allowing you to slowly reduce the percentage of consulting to in-house effort each year until substantially all of the work is done in-house. Particularly in the first year of compliance, there will be a lot of extra work that won't repeat in subsequent years. It may not make sense to build up permanent staffing levels for a temporary need. Co-sourcing can also provide a backup of knowledge, if either your in-house staff or outside consultants part company.
3. *Direct hire*
   A direct hire can be a cost-effective route, if you can find a prospective employee with the necessary experience and knowledge. As a result of this regulation there has been a flurry of hiring, both by companies, as well as various consulting and auditing firms. It may not be possible to find a quality employee with the skill set needed to manage and/or staff your compliance project. If you intend to go the direct hire route, you may want to consider promoting an existing employee or employees and then filling the vacancy(s). You may have a much easier time recruiting an accounting manager, senior accountant or an SEC reporting person than recruiting a 404 compliance manager. Another reason to hire from within relates to the learning curve. An employee who has worked for the company for a period of time will be familiar with the key players within the company and will generally have an easier time obtaining and evaluating internal information. One potential downside to the direct hire route is that your compliance staffing needs may not be constant throughout the year. Generally companies will have the highest staffing needs during the documentation and testing phases and during brief periods of ongoing testing.
4. *Utilize existing staff*
   If you have the capacity and knowledge, utilizing your existing staff can be an efficient and cost effective method. It may also mean working even longer hours and consequently

reduced morale. Before you decide on this method take a good honest look at your existing resources. Consider what other staffing needs might effect the time available to devote to this project. If your staff is already working long hours, unless you have a way to reduce their workload, it is unlikely that they will be able to successfully comply with 404. Assuming that you have the staffing capacity to bring this project in-house, you may also want to consider political ramifications. Will your existing staff be able to be objective about the Company and its internal controls, or will they let personal feelings effect their conclusions. They may have to report deficiencies in work performed by their peers or even supervisors. It could be potentially damaging if your own internal review gives you a clean bill of health, but serious problems are uncovered by the attestation work performed by your auditors. While there are a number of downsides to consider, utilizing your existing staff can be a great way for them to learn about other parts of the company and even do a little cross-training.

Ultimately, there is no one best way to staff this project. Each method has its positives and negatives. The key is to find the one that best fits your company's needs.

3. Timing and Compliance Schedule

Timing is extremely important in the first year of compliance. You will want to have the maximum amount of time to complete the project; however, if you take too long there will be little time to rectify any deficiencies identified internally or by your outside auditors. Consult with your outside auditors to determine the minimum period that a control must be in effect before you can begin testing. If that period is two months for example, you will not be able to begin testing until the third month.

Some basic parameters, that will work for many companies are:

- *Planning*: Completed by the first month of the compliance period.
- *Documentation*: Completed by the second month of the compliance period.
- *Testing*: Should be performed from the third month to the sixth month of the compliance period.
- *Remediation and Re-testing*: Should be performed from the seventh month to the ninth month.
- *Evaluation*: Completed by the ninth month.
- *Auditor Attestation*: Fieldwork completed by the tenth month; reporting completed by the eleventh month.

Conservative companies (or those that anticipate multiple deficiencies) should consider moving up the schedule to allow them time to correct potential deficiencies or other problems. You should also speak with your auditors about their timing as soon as possible. Can they commit to performing their attestation work at the scheduled time? If you can agree on a specific time, you will want to make sure that you are able to complete work that you are responsible for on time. If not and you are not ready at the scheduled time, you may have to take whatever time they have available. This might mean that they perform their attestation work so late in the

year that any deficiencies they find cannot be corrected and retested within the compliance year.

4. Framework Selection

In your annual report, you will be required to disclose which framework you used to evaluate your internal controls. While the final rules do not prescribe which framework to use, the COSO Framework is the best known. [3] In your planning section, we advise that you decide which framework you will use as it will affect the rest of your compliance effort. If you choose a framework other than COSO, be prepared to support that choice and demonstrate that it meets the requirements of 404.

As COSO is widely used, selecting another framework risks falling out of the mainstream. While another framework can be acceptable, validation or compliance using other frameworks is a subject that is beyond the scope of this white paper and is topic for discussion with your auditors. The rest of this document is based on the use of the COSO Framework. If you use a different framework you will need to research what is required by that framework.

5. Major Systems Selection

One of the most important things you must accomplish in the planning phase is to select your systems (sometimes referred to as "cycles"). A system can be very broad (such as purchasing/accounts payable/cash disbursements) or quite narrow (such as purchasing). In general, the larger the company the more narrow the systems should be. This is generally because large companies will have more departments that may be headed by different managers and located in geographically different areas. By comparison, a smaller company with a single administrative center may have systems that are quite wide.

To select your systems, begin by describing a list of potential systems. Now, look at your latest financial statements. Make sure that every line item in the balance sheet & income statement would fall under one of the systems. Add to your list as you go. Now look at the disclosures, make sure you know which system would include each of the significant disclosures. Remember that you are testing controls over financial reporting; therefore you want to make sure you cover all items that are material enough to be presented in your financials. Once again, this is another area that it will be important to obtain feedback and ultimately buy off from your audit committee and outside auditors.

6. Control Environment Assessment

In the planning process, you must assess the control environment. In our Tool, "Sarbanes-Oxley 404 Compliance Tool", we ask the user to self rate their company based on a series of questions designed to determine what level of risk exists within their control environment and sensitivity to that risk. Consider two companies: One company's stock fluctuates only within a fairly narrow trading range, management received less than 5% of their total compensation from bonuses and stock options, and the Board and Management have communicated their commitment to internal controls and accurate financial reporting all levels of the company. Another company's stock fluctuates widely on even the slightest rumor that earnings might be

off by a penny, management and most of the employees have pre-IPO stock options and track the stock price throughout the business day, and the company's CEO is known to get extremely upset if a department misses forecast. While both companies might have excellent internal controls, it is easy to see how the second company has a higher controls risk environment.

In considering the control environment, some areas to focus attention:

- *Incentives*: What are the incentives that might influence the decisions that management and employees make? How much of their salary comes from bonuses or incentive compensation? How important are stock options?
- *Staffing*: Does the company have adequate staffing? Are staff and management in appropriate positions given their background and training? Do they understand the significance of their actions? Is there a morale problem?
- *Internal Controls*: What is senior management's attitude towards internal controls? How does this get committed to others within the company? Do the employees view management as ethical?
- *Outside influences*: What role do stock analysts play? Is the company under significant pressure to report certain results? How significant are debt covenants? Is the company trying to raise capital?

Once you have considered all of these areas, you will want to determine the company's overall risk level. In doing so, you should compare yourself to other public companies. We advise against strict comparisons against other companies in your industry. You might be more or less risky than others in your industry. If for example, you consider your industry to be high risk, you might incorrectly conclude that you have an average or low risk control environment by comparing yourself to your peers. Whatever you conclude, you should produce some support to back up your assessment. This need not be more than a memo in the file documenting your conclusion and the factors you considered. Your assessment of control environment should then factor in to the level of testing to be performed. The higher the risk in the control environment, the tighter your internal controls should be and the higher the level of testing.

7. Test Planning

In your planning, you should lay out a methodology of how you intend to test your controls. You will want to find a way to ensure that controls are tested consistently based on their importance to the company. This is especially important when multiple parties are performing the testing. Imagine one team member making three selections to test a control over revenue recognition, while another team member makes one hundred selections to determine if controls over petty cash are functioning effectively. If you don't lay out guidelines, this can and will happen.

The end goal of your test plan methodology is to provide a "Reasonable assurance" [4] that the controls over financial reporting are effective. Some things you will want to consider:

- How much testing is enough? How will you treat controls over significant (or material) risks, how will you treat controls over risks that are likely to occur. Will you make more selections for likely and significant risks than unlikely and/or insignificant risks?
- What should the minimum sample size be? You will need to decide on a minimum number of selections for testing (25 samples is considered a reasonable number of selections as a starting point but more selections may be required for high risk areas depending upon assessed significance and likelihood).
- How will you handle testing small populations? You will need to decide how many selections make sense for a given control.

You will need to find a way to correlate materiality to your level of testing. In our Tool, we base sample size on the significance score (materiality), the likelihood score (inherent risk), and the assessment of the control environment. You will also want to define a methodology for making consistent selections. If you allow the tester to choose which selections to test, you run the risk that their sample is not representative of the entire population (i.e. they picked only the items for which the control was functioning and skipped over items which might indicate a deficiency). We provide a tool that statistically selects a sample based on sample size, population size and a calculated random number. However, you can design your own system as long as it is consistently applied. The system need not be complex. It should however remove the tester's discretion to select which items to test.

One last area to consider is testing schedule rotation plans (performing testing every other year or longer for risks assessed to have low significance or likelihood). We believe that for risks that are relatively insignificant or unlikely, rotation plans can be used effectively. This will reduce the amount of effort expended on lower risk areas allowing you to focus on other testing. However, your auditors will ultimately determine if you have performed enough testing to properly assess the company's internal controls. As a result, if you are considering using rotation plans in the future, you should seek your auditor's approval prior to doing so. It should also be noted that all controls should be tested in the initial year of compliance. The use of a rotation plan would only apply to subsequent years, after the control had been tested and found to be effective

8. Major Systems Documentation

Once you have completed the Planning stage, you will want to begin the Documentation stage of compliance. Each of the systems that you identified in the planning phase must now be documented in detail. We recommend beginning the Documentation effort by collecting information about each system in as much detail as possible. Focus on gathering the essential aspects about the system that would allow an outside accountant to fully understand the system. Some things to consider are:

- Management of the department or function
- Significant employees and their functions
- Key reports or other output of the system
- Goals or objectives of the system
- Workflow

- Exception handling
- Key system controls
- Risks and opportunity for fraud or material misstatement
- Areas of potential control breakdown

Along with the gathered information, you will want to include additional documentation. This documentation could include:

- Key employee Resumes'
- Key reports
- Reporting structure
- Policies & procedures manual
- System questionnaires provided by your auditors
- Existing Controls documentation and/or workflow
- Prior control failures or process breakdowns if any

This documentation will be used each year and only updated for significant changes. As a result, if you do a thorough job the first year, you will get the benefits for years to come.

9. Feedback and Communication

Throughout the Planning and Documentation phases, feedback and communication will be important to the successful implementation of 404. If you have not started planning yet, meet with your auditors to let them know that you are beginning the process and seek out any feedback or comments. They may provide you with samples obtained from companies farther along in the process. Once you have met with your auditors, begin formalizing your written plan. Once you have an outline of the plan, seek feedback from management, and your auditors. Once you have updated the plan to include their feedback, you can forward it to the audit committee. You may also want to send a copy to the full board of directors.

Once planning is completed, consider how you will communicate the plan to all the team members and outside consultants, if any. You may want to set up a meeting schedule, both with your team as well as a separate meeting with the auditors so that they will be informed as to how the project is progressing. How frequently you meet will depend on the complexity of the company and the nature and frequency of deficiencies. You may also want to consider how to communicate the project with the rest of the company. They may be asked to participate in some way and should be aware of the importance of the project to the company.

Feedback and communication is extremely important if problems come up during any part of compliance. We recommend that you address and communicate all issues as soon as they are identified. Issues don't tend to go away, and it is in everyone's best interest that they be identified and addressed as soon as possible. This is especially true if your schedule is slipping and you have missed deadlines. We believe that most problems can be resolved if they are dealt with in an open and honest manner.

10. Next Steps

Once the Planning and Documentation phases are been complete, you will be ready to move on to the testing phase. Both testing and the evaluation process will be addressed in depth in our next whitepaper: 'Sarbanes-Oxley 404 Testing and Evaluation.'

Conclusion

The Planning and Documentation phases form the foundation for SOX 404 compliance and are the key to a smooth execution for ongoing years. Fully planning for the compliance process and gathering and documenting the important details about your company are the first step towards compliance. Communication of the plan and the documented systems during this effort will prepare your team and your company for the next phases of compliance. Feedback during this period with your auditors, board and your team members should catch problems early enough in the process to allow timely correction and successful compliance. Acquisitions of privately traded companies will require revisiting the planning and documentation activities but should integrate with the existing work if done properly.

References

[1] SEC Release 2003-66
[2] Whitepaper: A Framework for Evaluating Process/Transaction-Level Exceptions and Deficiencies October 28, 2004, Representations by 9 Large Audit firms.
[3] May 29, 2003 speech by Scott A. Taub, Deputy Chief Accountant of the SEC
[4] COSO Framework Definition statement.

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.