July 2006

Sarbanes-Oxley Section 404 Testing and Evaluation

Applying the COSO Framework: Using a Top-down Risk-based Approach

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. Information regarding Planning and Documentation can be found in the Whitepaper 'Sarbanes-Oxley Section 404 White Paper: Planning and Documentation'. This whitepaper provides more in-depth guidance regarding implementing the Act: specifically the Testing and Evaluation requirements.

1. Why use a Top-down Risk-based Approach?

A top-down approach is one that originates at the financial statement level and drills down to financial statement line items, GL accounts and then individual transactions. Traditional financial audits (such as the annual audit all public companies have) are generally bottom up. This means that transactions are tested and traced back to a posting in the general ledger. General ledger accounts are aggregated on a "lead sheet" and lead sheets are traced to the Company's financials statements.

A risk-based approach is one that considers risks first, then seeks to identify controls to mitigate the risks and finally tests the controls to make sure that they are sufficient to mitigate the identified risk. When you think about it, it makes perfect sense -- why do we need a control if no risk exists? A risk-based approach also adjusts the scope and level of testing based on the underlying risk.

According to the SEC:

> *Both management and external auditors must bring reasoned judgment and a top-down, risk-based approach to the 404 compliance process. A one-size fits all, bottom-up, check-the-box approach that treats all controls equally is less likely to improve internal controls and financial reporting than reasoned, good faith exercise*

> *of professional judgment focused on reasonable, as opposed to absolute, assurance.* [1]

Why would you use this approach? First of all, a risk assessment is an integral component of the COSO framework. Secondly, it is a more efficient methodology, that allows for a Company to more accurately identify and test controls that are critical to accurate financial reporting.

According to COSO:

> *A risk-based approach can bring significant efficiencies to internal control assessments.* [2]

It allows you to identify those areas where the most risk exists and pinpoint testing. Starting from the transaction level generally results in excess testing.

In recent communications, the SEC has made clear their preference for this approach:

> *Commentary submitted to the Commission has suggested that management assessments under Section 404 have not fully reflected the top-down, risk-based approach the Commission intended. Building from the information gathered in response to the Concept Release, and from the anticipated COSO guidance, the Commission currently anticipates that it will issue guidance to management to assist in its performance of a top-down, risk-based assessment of internal control over financial reporting. To ensure that this guidance is of help to non-accelerated filers and smaller public companies, the Commission intends that this future guidance will be scalable and responsive to their individual circumstances.* [3]

2. Assessing Risk

After you have documented the major systems (or cycles) you will need to assess risk. This can be done by breaking up the system into steps or components. For example, the Disbursements system might include the following steps:

1. Purchase order approval
2. Good or service is ordered
3. Good or service is received
4. Vendor submits invoice
5. Invoice is approved and coded to appropriate GL acct
6. Invoice is input into accounts payable
7. Check is printed
8. Check is signed
9. Payment is mailed and accounts payable relieved

For each step in the system different risks are present and should be identified. For example, in the first step 'purchase order approval' one risk might be that 'an employee exceeds their

purchasing authority'. Another risk might be 'that orders are placed without verifying that an approved purchase order is on file'.

Other steps will have a very different set of risks. For example in the step, 'invoice is approved and coded to the appropriate GL acct', one risk might be that 'the invoice is improperly coded'. The risks should include everything that could potentially go wrong which might lead to a fraud or misstatement. For each step there may be multiple risks.

3. Evaluating Risk

For each risk on the list, you should evaluate the risk. The evaluation should include an assessment of frequency as well as an assessment of the significance. Frequency implies how likely is it that this type of problem may occur. Significance relates to financial materiality, but is more broadly interpreted to include damage to reputation and other intangible impacts. Fraud by senior management, might not be material per se, but could have a significant impact on the way that shareholders view the company.

Frequency and significance must be considered in tandem. In the previous section, we discussed a potential risk that an invoice was improperly coded. This might happen quite frequently, but unless there is a pattern (such as improperly classifying expenses as fixed assets) it is unlikely to be significant.

According to COSO:

> *Risk-based means focusing on quantitative and qualitative factors that potentially affect the reliability of financial reporting.* [3]

4. Mapping Controls

When you have identified risks for each step within each discrete system, you will need to begin identifying mitigating controls and mapping them to the underlying risk. For example, with the risk that 'an employee exceeds their purchasing authority' a mitigating control would be that 'accounts payable verifies that the purchase is within the signer's authority prior to payment'.

Controls can be preventive or detective. 'Locking up blank check stock' is an example of a preventive control as it prevents unauthorized parties from gaining access to the company's checks. The control 'accounts payable verifies that the purchase is within the signer's authority prior to payment' is a detective control. At the time accounts payable verifies the approval level the purchase has already been made, so it does not prevent it from occurring. It does detect it shortly after it has occurred and the timely detection has the effect of deterring the action.

Just as there might be multiple risks per step, there may also be multiple controls per risk. It is easy to see how with multiple systems, each with multiple steps, that in turn have multiple risks and multiple mitigating controls, simply documenting and organizing this process is an

enormous task. Prior to starting the documentation, you should have a system in place that fits the size and complexity of your organization.

Our Sox 404 Compliance products are designed to meet the needs for a wide variety of companies and we provide tools to address varying levels of complexity.

Certain very large organizations may need a sophisticated custom system while organizations with more straightforward requirements may get by without a formal system. The important thing is that you assess your needs and find a system that is appropriate.

5. Identifying Gaps

After controls have been identified and mapped to the risks, certain gaps will exists. Principally, these are risks for which no control exists. In this process you will also need to determine if the design of the control(s) is sufficient to mitigate the risk. You may have controls that, after further examination, are found to be inadequate. Risks without controls and risks with inadequate controls, should be prioritized and addressed.

Considering the frequency and significance factors of the underlying risk, you will begin by designing and implementing controls as needed. If time permits, address these issues prior to starting the actual testing. If time does not permit, correct the most significant gaps and then begin testing. Less significant gaps can be addressed concurrently.

6. Testing Controls

For each control identified, design a test to determine if the control is working as designed. In doing this you will need to identify a population and a time period. For example:

System: Disbursements
Step: Check is signed and accounts payable relieved
Risk: Large dollar check issued erroneously
Control: Two authorized signatures required for checks in excess of $5,000
Test: Select checks issued in excess of $5,000 and obtain cancelled check and verify that there are two signatures and each is an authorized signer
Population: Debits to accounts payable in excess of $5,000 from 1/1/07 to 6/30/07

It is important that the test of each control is designed to determine that the control is working. The goal here is not to duplicate work already performed by the outside auditors in their regular financial audit. Using the previous example, a selection was tested and found to only have one signature. The underlying payment was a true and legitimate payment. For the regular year end audit testing, the item would not be considered an exception (as it was a legitimate payment) for SOX testing the item would be considered an exception as the control was not functioning as designed (as there was only one signature when there should have been two).

The testing workpaper should include a detailed listing of each item selected for testing and the results of the test. The auditors will need to review this documentation, and will re-perform a percentage of management's work.

The number of selections and the methodology for selecting them is not specified by the SEC. Our SOX 404 Compliance products, use a formula that determines sample size based on population size, likelihood score, significance score and an overall company-wide control assessment. Selections are then made based on fixed intervals throughout the population. Companies should strive to achieve a consistent methodology and to develop a sample selection that does not allow the tester discretion to pick selections. The outside auditors, in addition to re-testing management's work will make selections that were not part of management's sampling. Testing exceptions identified in their work but not reflected in management's work could cast doubt on the integrity of the compliance effort.

We should remember that the COSO Framework indicates that we are seeking reasonable assurance (and not absolute assurance) that the control is working as designed.

According to the COSO Framework:

> *An internal control system, no matter how well conceived and operated, can provide only reasonable--not absolute--assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs.* [4]

A key concept in a risk based system is to correlate the level of risk with the level of testing. In the first year of SOX implementation, far too much time was spent testing large numbers of routine transactions for which an error was unlikely to have a significant impact on the company or its financial statements.

7. Remediation

Remediation is required when a control is either not designed correctly, or is not functioning as designed. A testing exception (as described above) is usually indicative that the control is not functioning as designed. Remediation entails performing corrective action and then both re-evaluating the control and then re-testing it. The new control must be both designed correctly and functioning as designed.

The new test can be the same as the original test or can be changed if the underlying control has been modified. In many cases, testing failures are a result of employees not following policy or of policies not being clearly communicated to the employees who use them. If this is the case, remediation may be as simple as holding a meeting with the employees involved, training them on the policy and letting them know that they will be held accountable for any policy deviations in the future.

Timing is a key consideration in the remediation process. After a testing failure is identified, it will take time to put corrective action in place, then those actions must be in place for a sufficient period of time before they can be re-tested. Transactions during that period of time become the new population and the test is re-performed. Specific attention should be paid to controls that are performed quarterly (compared to controls that are transaction related or monthly). If the population includes the first and second quarters, and a test exception is identified remediation would need to be in place prior to the third quarter in order to re-test the third quarter. Regardless of the frequency of the control, it is important to discuss with your outside auditors to define the minimum amount of time needed after remediation before a control can be re-tested.

In the initial compliance year (and even sometimes in subsequent years), there may be more controls that require remediation than time remaining to correct and re-test the deficiency. In that case, deficiencies should be prioritized and those which are considered significant and highly likely should be addressed first.

8. Evaluating Results

As the compliance year draws to a close, you will need to evaluate the results. Our Sox 404 Compliance products help the user aggregate and evaluate any deficiencies remaining. We consider deficiencies in risks that are both significant and likely to be potential material weaknesses.

We consider deficiencies in risks that are either significant but not likely or likely but not significant to be potential significant deficiencies. Deficiencies that are both unlikely and insignificant are considered potential deficiencies. After considering the number of potential material weaknesses, significant deficiencies and deficiencies, management must conclude if material weaknesses exist. A material weakness can exist as a result of one extremely significant deficiency or can be the result of numerous less significant deficiencies.

Regardless of the evaluation method used, we would anticipate that the conclusion would be made in the context of open communication with the auditors.

9. Next Steps

Once the Testing and Evaluation phases are complete, you will be ready to include management's attestation in your annual report. The form of that report will be dictated by your conclusion as to if a material weakness exists. If you have concluded that a material weaknesses exists, it must be appropriately disclosed in your annual report.

Once this is done, you are ready to move on to the next years testing. If time permits, you may want to address any remaining deficiencies before beginning the next year's work.

Conclusion

The Testing and Evaluation phases are the heart of SOX 404 compliance. Understanding what is required and prioritizing based on risk can make the process more efficient and eliminate unnecessary effort.

References

[1] SEC Release 2005-74
[2] COSO: Internal Control over Financial Reporting – Guidance for Smaller Public Companies
[3] SEC Release 2006-75
[4] COSO Framework - Executive Summary

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.