
From: Gorman, Denise [DGorman@hineshort.com]
Sent: Monday, April 24, 2006 8:04 PM
To: Comments
Subject: Internal Control Roundtable

PCAOB/SEC Roundtable:

I have been employed as an external consultant assisting public filers with SOX readiness since 2004. I have worked with both accelerated and non-accelerated filers in various industries.

Based on my observations, I am writing on behalf of my present, former, and future clients to request that the Committee consider some or all of the following during the codification of ASx:

Consider putting primary focus on the following areas:

1. Monitoring controls in the recording and reporting process. The management review of journal entry input, SEC supporting work papers, and draft SEC documents are the final controls over financial reporting to ensure that the documents are compliant, complete, and error free. Transactional controls are of lesser importance if the final monitoring controls are working effectively. Also, monitoring controls are more cost-effective and usually operating reasonably well prior to any SOX effort. Remediation cost of monitoring controls is usually less costly.
2. Communication to Audit Committee. Effective management override controls, whistleblower controls and code of conduct certifications are the most important entity level controls to ensure that management operating style and communication is COSO compliant. Other entity level controls should be recommended but not mandatory.
3. Board of Directors Governance. Best practices should be scaled for the size and composition of the Board. Guidelines should address stock exchange requirements but limit any additional best practices within reason. For example, documentation of meeting agendas and discussions are likely to be less formal in a smaller public company.

Consider the following to assist the smaller public companies in reducing the assessment/remediation cost and level of resources:

1. Scale back COBIT compliance testing to necessary levels. Provide smaller public companies with the option of outsourcing the management assessment and testing. The use of a third party's General Computer Controls Review accompanied with proof of remediation by management for issues identified should be a sufficient level of testing. Documentation of internal policies and procedures should be required for applications change management, logical access to significant systems and key spreadsheet network files. Documentation of other IT internal controls and policies/procedures should be recommended but not required if management can justify that additional documentation is not cost-effective.
2. Evidence of Approvals and Authorizations should be limited to the following:
 - a. Significant capital appropriations as defined by company policy. If no policy exists, consider a percentage of total capital expenditures in the audit period.
 - b. Significant purchase agreements, other than contracts or leases requiring officer's approval.
 - c. Significant cash transactions as defined by company policy.

- d. Non-standard, non-routine journal entries only. Recurring or routine journal entries should not require evidence of approval due to mitigating monitoring controls such as management's review of the trial balance and financial statements.
3. Separation of duties should only be required in specific situations where alternative controls do not exist. Small staff sizes make it impossible to separate authorization, physical possession, and recording duties. If alternative monitoring controls exist, consider that the separation of two of these three functions is sufficient.
4. Set limitations on scope of audit for significant sites based on cost/benefit. It is not uncommon for a smaller public company to be a multinational with numerous sites. Significant site determination should be determined by balance sheet & income statement matrices, existence of previous control issues, and cost of conducting an audit in multiple sites. The external auditor should consider the cost impact on an organization to reach a 60% matrix threshold and in instances where the total estimated cost of management's assessment exceeds a threshold (see item #2 below); the 60% threshold should be relaxed to prevent the scope of audit from eliminating profitability or liquidity.
5. Limit re-performance of transactional testing to anti-fraud controls or areas of previous internal control issues. Rely on the work performed by others to a great extent for transactional controls. There are usually monitoring controls to compensate if these controls do not operative effectively.
6. Relax timeframes for update testing. Smaller staff sizes at smaller public companies result in only a handful of employees available to assist in the testing of control effectiveness. Allowing the smaller public companies to spread the testing throughout the audit year will reduce the cost of hiring temporary staff in the later part of the year to support normal peak workload and extra demands from SOX testing.
7. Publish statistical guidelines for audit samples rather than firm guidelines. Smaller companies have less volume of transactions than larger public companies. Consider setting number of test transactions based on population size as well as frequency of control would reduce audit sample size and cost of testing.

In developing the ASx, please the following to improve the first year implementation at smaller public companies:

1. Publish guidelines for reliance on the work of others ASAP. Timely clarification of division of responsibility between internal and external auditors assists both auditors to plan a more effective audit. Project plans can be developed more effectively with early notification.
2. Publish guidelines regarding cost-benefit analyses for scope decisions ASAP. Creeping scope was a costly, unexpected obstacle to accelerated filers. Requiring that external auditors concur on scope of management's assessment early in the audit year will allow management to plan a more effective assessment plan. Obviously, scope can be adjusted by the external auditors for audit risk, as appropriate. Early assessment should be based on the auditor's assessment of audit risk from the 2006 financial statement audit. Cost of incremental scope should be based on percentage of net income or cash flow from operations, with a not to exceed limit if the cost of SOX implementation impacts the company's liquidity, creates a loss situation for an otherwise profitable company, or creates a situation whereby debt covenants would be violated. The audit report should be allowed to address and explain this scope limitation.

For future years, consider inclusion of the following in ASx:

1. Limiting management testing performed on a risk based analysis. It is anticipated that the cost of compliance will not drop off in future years at the same pace as accelerated filers. In many

instances, controls operated effectively in prior testing and there has been no change in procedures or staffing since the last assessment. Consider a two or three year rotation of management assessment for instances of low risk on transactional testing.

I appreciate this opportunity to provide input on behalf of my clients.

Respectfully submitted,

Denise Gorman, CIA, CMA, MBA
Resources Global Professionals
Audit Services