April 28, 2006
Request by SEC and PCAOB for comments on SOX 404 lessons learned

I appreciate the opportunity to provide input for enhancing the efficiency of implementing internal controls over financial reporting assessment, pursuant to Sarbanes-Oxley Section 404. I am the SOX Compliance Manager at 3M Company, a Fortune 500 company with revenue in excess of $21 billion.

In general, I believe that well managed companies have been performing the key controls to ensure accurate financial reporting and safeguarding of assets, and understand and support the intent of SOX 404 to protect the investor by providing evidence of such control effectiveness. As a company in the third year of compliance, I see the progress thus far and also see the need to further enhance the regulatory guidance to help reduce the burden of compliance. I have the following suggestions for your consideration.

- Enhance the guidance and amend AS2 language on
  - Risk assessment and integrated audits
  - Safeguarding of assets
  - Information technology
- Provide a framework for companies to leverage
  - Entity level governance controls
  - Prior year results
  - Continuous testing
  - Management testing

Enhance the guidance on Risk assessment and integrated auditing
Today an external auditor is required to test a certain amount of transactions for SOX and for financial audit**.** While the PCAOB has indicated that the scope of work for Section 404 should be focused on areas where there is a possibility of a material misstatement, the same should be said about the scope of the whole integrated audit. As indicated in AS2, auditors continue to include areas in scope that are highly unlikely to be the source of a material misstatement. I would like to see quantitative guidance on risk assessment process that can be used by the company, the external auditor, and the PCAOB. If a regulator isn't clear on how it will judge whether a company has done an acceptable job of determining risk, companies (and external auditors) must do more work to ensure they have covered all possible areas they might be tested on. There is no incentive for companies to avoid raising the bar beyond what the legislation was intended to address.

Enhance the guidance on Safeguarding of Assets: There is not a consistent understanding of fraud risk relating to safeguarding assets that should be considered. While guidance is clear on frauds (or thefts), it is not as clear for this portion of the internal control definition relative to "receipts and expenditures are being made only in accordance with authorizations of management and directors of the company." Should the focus be on a risk of material misstatement of the financials? Should it be at an executive management level, mid management level, or each employee? The current example where the PCAOB has focused on segregation of duties is at a very low level with a focus on operators and administrators of transactions.

Enhance the guidance on Information Technology (IT)
There continues to be a significant amount of bottom-up risk identification, especially when determining what IT General Controls should be in scope. There is significant variability among external audit firms and among filers. The IT infrastructure and its variability from one global ERP instance to unique, decentralized IT environments is one key factor in the differences. 3M's plan is to focus on SOX critical applications in scope for business IT controls and support IT infrastructure associated with these SOX critical systems in scope for the technical IT controls. There does seem to be a need to find a balance between the automated controls and level of testing needed vis-a-vis other mitigating controls and testing of those controls. Often, for SOX and financial audits, these are tested by different groups within the external audit organization which can result in differing expectations. Taking that point further, both management and the external auditor need guidance on what constitute key controls within IT General Controls. How does management or the auditor continue their top-down risk-based assessment from significant accounts to individual IT General Controls? Additional guidance on standards which can be leveraged when centralized or standardized IT applications and infrastructure exist would be very helpful in optimizing testing. Additional guidance on leverage of integrated IT testing is desired.

Provide a framework for companies to leverage entity level governance controls
While companies have identified and tested controls which evidence the control environment, the ability for external auditors to rely on them is still subject to what seems to be a variety of interpretations and determination by each firm. Guidance on acceptable ways to leverage these governance controls in the risk assessment, with the objective to reduce duplicative testing, is desired.

Provide a framework for companies to leverage continuous testing
The current guidelines suggest that the majority of SOX testing needs to occur near the fiscal year-end. We would prefer to see support for companies which have more frequent testing processes (e.g. quarterly) to allow external audit testing throughout the year to reduce the burden (and cost) at year end. Testing at year end allows limited time for remediation. This seems inconsistent with the goal for early detection and resolution, continuous improvement of control environment, and investor protection. Stock is bought each day – why not encourage timely testing and remediation?

Provide a framework for companies to leverage prior year results
A critical component of risk assessment is knowledge of past result and areas of change in people, process, or systems. Today, a significant portion of the SOX burden is driven by external auditor testing of controls. Where past results indicate effectiveness and no change has occurred, consideration should be given to allow reduction of the level of testing required.

For example, let's say that the current level of testing is 100. If historical testing was effective, but changes in people, process or system occurred, the level of testing could be reduced slightly (e.g. to 75) with a focus on the areas of change. If historical testing was

effective and no changes occurred, the level of testing could be reduced significantly (e.g. to 25). This would enhance the perceived value of SOX by aligning effort with return.

Provide a framework for companies to leverage management testing and test the process rather than testing the controls

A key assumption in testing is the concept of independence. SOX 404 states management must identify, assess and monitor the effectiveness of controls over financial reporting. In addition, the external auditor must opine on the design and effectiveness of controls. Their opinion is based on re-testing of controls. Where a company has management testing performed by someone other than the person performing the control (there is independence), and where entity level controls are tested and effective, a large burden of SOX could be relieved if the external auditor were able to test the management process and opine on the process, rather than the controls. Last year, we had a situation where we identified ineffective controls early in the year (first quarter), we fixed the problems in second quarter (retesting showed the control was effective), and considered it remediated in third quarter (tested and found effective again.) This was the company's assessment. Because the external auditor didn't test that control (it wasn't in their risk assessment), it was considered deficient. Time spent on evaluating such items is non-value adding. It would add value to allow the external auditor to provide an opinion on the company's process for resolving issues (e.g. we have corporate audit re-test a sample of controls to provide assurance over our process.) This way, companies aren't penalized for doing more testing or more frequent testing.

I appreciate the opportunity to provide input and look forward to seeing the comments and suggestions integrated into future communications.

Diane Allen
3M Company
dsallen2@mmm.com
651-733-1633