From: Paige Easley [mailto:paige.easley@gmail.com]
Sent: Sunday, February 25, 2007 10:33 PM
To: Comments
Subject: Comments on proposed standard

Dear Sir or Madam:

After reading "PCAOB Release No. 2006-007, December 19, 2006", I would like to make a few comments.

Overall I agree with the changes that are suggested, specially the risk based approach for companies and the understanding that smaller companies may have different risks.

I have two areas of concern that were not mentioned in the release, they are:

- A base set of standards (for both IT and Finance) should be published by the PCAOB
- That the idea of point of time review should be reviewed to include those failures in controls though out the year should be counted as a deficiency even if it has been remediated.

Base set of standards - I realize that not all controls are key controls and not all key controls would be key controls for all companies. But, I would put forward that there are several key IT and Finance controls that would always be key for any organization and thus the PCAOB should outline them just as the OCC and OTS does for the banking industry. Examples of these type of key controls would be passwords on all in-scope IT applications and review of and balancing of financial information.

Point-in-time - In conversation with both the SEC and PCAOB representatives I have been told that the SOX audit is a point-in-time audit and even if a controlled had failed earlier, if it had been remediated and then tested successfully you would not note the earlier failures and there would be no deficiency. I disagree strongly with this presumption that the SOX audit should only be a point-in-time and these corrected deficiencies should not be part of the final report or used in determining control effectiveness. Thus, a company's key financial system could have had no passwords, logging, reviewing of infractions for the first half of the year, then be remediated and passed because passwords were turned on the second half of the year. The sample sizes used to determine operating effectiveness are not large enough to find any type of fraud, material mistakes when there is the ability to delete transactions without a trace, be the requester, approver and reviewer of a single transaction, to have anonymous abilities to enter, change or delete data without a trace can not be ignored. I propose that when deficiencies are found in a key control, it will be reported on and used in determining the overall risk at the end of the year, even if it has been remediated. I have found that second and third year companies are the ones most likely to completely ignore the control set for the first half of the year and then only in response to the internal audit review do they take any action to remediate the key control that was noted as deficient.

You ask in question number 6 "Would the performance of a walkthrough be sufficient to test the design and operation effectiveness of some lower risk controls". I would say no, since in my experience what I have been told in a walk through is often not what occurs. What I would suggest is that for low level risks that the sample size be made much smaller (in the 3 to 5 range).

Your comment about "Auditor's Attention Towards the Most Important Controls" is justified, but I would go farther in stating that the attestation auditor must provide a risk analysis showing why they have added key controls that the company being audited for compliance had not identified. The reason I believe this is important is that every single attestation firm as given me a list of controls and told me they were key without ever do any risk ranking to determine if the controls are truly key, important or even exist.

Thank you for your time.

Paige M. Easley
Partner
LP Risk Services, Inc.

(310) 897-3684