11/19/2012

Public Company Accounting Oversight Board
Attention: Office of the Secretary
1666 K Street, N.W.
Washington, D.C. 20006-2803

PCAOB Rulemaking Docket Matter No. 37
Concept Release on Auditor Independence and Audit Firm Rotation

Dear Chairman Doty and Board members,

Information security professionals have observed the widespread lack of independence, objectivity, and professional skepticism in the public accounting profession since the passage of the Sarbanes Oxley Act (SOX) in 2002.

SOX greatly increased the third party service provider assurance market for service auditors, as publicly traded company issuer auditor and management demand for internal controls over financial reporting (ICFR) increased. The Statement on Auditing Standards no. 70 (SAS 70) report was widely used to demonstrate a service organization's defined scope of internal controls which often produced a report that provided ICFR opinions for AU Section 324 mixed with (or entirely comprising) non-ICFR criteria and testing to support security, availability, processing integrity, confidentiality, and privacy (SAPICP) principles, and other attestations as a "catch-all" services provider audit standard.

The misuse of the SAS 70 standard beyond ICFR was acknowledged by the public accounting profession in 2010, with the AICPA produced AT 801 standard, updates, and retirement of the SAS 70 standard in 2011. Statement on Standards for Attestation Engagements no. 16 (SSAE 16) with ICFR opinions was produced, and a guidance for Service Organization Control (SOC) report formats with management assertions segregated ICFR objectives, controls, and opinions from non-ICFR. However, ICFR opinion misuse continues with use of non-ICFR criteria and tests, because the root causes of the misuse were not acknowledged and addressed properly. The misuse contributes to a false sense of security on the part of uninformed users who place misguided reliance on the reports, and diminishes the value of third party attestations.

The root causes of the misuse are grounded in lack of independence, objectivity, and professional skepticism and include:

1) Inadequate investment in issuer management and auditor financial reporting risk assessments and evidence planning to justify and communicate timely a need for internal and external services provider ICFR report. The result is an issuer's demand of a service provider, without a communication of any issuer financial report accounts deemed high risk and objectives in need supporting evidence.

2) Issuers and their auditors are incented to demand service organization reports inappropriately as free "filler" substitution for inadequate ICFR continuous monitoring controls and to reduce issuer auditor ICFR evaluation cost.

3) Issuers, truly unable to manage the potential for financial statement reporting material inaccuracies without a service organization's assistance, do not communicate the reliance nature of the need contractually for clarity, or discuss and negotiate the obligation appropriately. Some issuer agreements state that "a SAS 70 must be produced annually" as the total direction, leaving a service provider to guess why an audit is needed.

4) Service providers in a vacuum, create a "best guess" audit scope in hopes of providing value, and select a non-ICFR criteria framework to support that scope. Non-ICFR criteria (such as SAPICP) enable service organizations to assert their self-defined information technology-related controls have been validated, but these tests and criteria are not designed to support a financial reporting opinion.

5) As reported by PCAOB quality reviews, public accounting firms and issuers continue to use service provider reports without appropriate ICFR criteria. The lack of objectives definition and formal contract negotiation often provides no effective ability to enforce a specific scope or new responsibility on a services provider. Other than the PCAOB's reviews, there is no consequence when issuers or issuer auditors receive a faulty service non-ICFR organization report to change the behavior.

6) Under pressure from issuer auditors asking for an undefined ICFR report, and a service provider requesting a non-ICFR framework scope, the service auditor is more likely to appease the client by using the service provider's non-ICFR scope for testing, and issue an ICFR opinion letter.

The misuse of these reports could have been easily prevented if the issuer public accounting firms would have followed their professional standards, performed proper risk assessments, and communicated valid financial objectives needed in a timely manner, or at least issued limited scope financial reporting opinions as a result. Instead, public accounting firms chose to ignore their professional standards en masse, demonstrating a lack of independence, objectivity, and professional skepticism.

It is true that ICFR controls are not easy to define universally, are dependent on individual circumstances, and are subject to identification through auditor judgment. This is why the professional standards make allowances for auditor judgment. However, the standards subject auditor judgment to a reasonableness test, and the majority of these reports contain controls that fail that test.

This problem is especially apparent with data center, managed IT services, and cloud service provider industries, whose operating personnel are highly unlikely to have any financial reporting controls capabilities, or be able to do anything to help a customer having any financial reporting crisis. Any objective non-financial reviewer familiar with information technology can randomly select one of these

reports issued to a service organization in these industries, and have a high likelihood of observing the failure of the ICFR reasonableness test: an ICFR opinion with non-ICFR criteria testing. Also, access to the contracts will also evidence they have not accepted financial reporting responsibilities, yet service auditors require providers' management to sign financial reporting assertions.

In the worst case scenario, IT security breaches occurring while under the management of an IT services provider, would be detectable via appropriate issuer financial statement reporting monitoring and reconciliation controls. In addition, the issuers should have control designs to self-verify authorized use of financial system reporting access accounts and logs without help from these types of providers. Typical examples of non-ICFR controls provided by these services providers and service auditor reports include, but are not limited to:

- Environmental controls such as having a diesel generator for backup of commercial power, raised flooring to provide better ventilation and cooling, the existence of fire suppressant mechanisms, water sensors, air conditioners, uninterruptible power supply (UPS) units, etc.
- Human resources related controls such as background checks, attendance tracking systems, employee handbooks, annual employee reviews, etc.
- Operational controls such as the existence of help desk ticket systems, server service state and performance monitoring software, the availability of technical support personnel, escalation procedures, DDOS protection and mitigation, etc.
- Most physical security controls, and hardware related logical access and change management controls are non-ICFR as well because of number of controls that would also have to fail in order to cause a client misstatement of their financials.

My detailed analysis of actual controls from anonymized service auditor reports showing why the controls are non-ICFR will be provided to The Board upon request.

In many situations, it is clear that the service auditor should not have issued one of these reports at all. For example, a simple online search on the keyword "SAS 70 certified" and "SSAE 16 certified" reveals examples of companies in industries with no apparent ability to impact their client's financial statement accuracy whatsoever.

- Online Voting Solution Providers (eBallot)
- Electronic Health Record / Electronic Medical Record Providers
- IT Helpdesk Outsourcing Companies
- Data Recovery Service Providers
- Website Development Companies
- Advertising & Marketing Companies
- Etc., etc.

It is difficult to overstate the negative effects that the misuse of SAS 70 and SSAE 16 has had on the security industry. In October 2011, The SEC expressed that IT security must be considered in an issuer auditor's risk assessment, as IT security breaches are known to lead to material impacts on reported

legal costs and revenue in financial statement balances. The focus of these hearings, however, is not to confirm that there is lack of independence, objectivity, and professional skepticism in the public accounting profession, but rather, having already concluded that it exists, the PCAOB seeks to determine what should be done about it.

In previous public roundtable hearings, and in comment letters, individuals have asked the PCAOB to provide examples of lack of independence, objectivity, and professional skepticism it has observed so that points of failure could be identified, and addressed. The PCAOB is prohibited from exposing details of its inspections by statute, so I offer the following analysis of the widespread service auditor report misuse to show where two of the greatest independence, objectivity, and skepticism failures have occurred. I also offer my recommendations for implementing controls that can prevent these failures from occurring in the future.

The single greatest point of failure in the area of service organization reporting is the failure of user (issuer) auditors to acknowledge issuer management's vendor oversight control deficiencies, when service auditor reports that address non-ICFR controls are used for management's ICFR assertions. A service auditor's inability or reluctance to follow professional standards may demonstrate a potential lack of independence and reduced validity of the results, especially as a secondary review occurs to release reports. User auditors should also reduce the reliance on such a report for audit risk assessment and reduce any partial substitution planned for direct independent testing, in order to maintain their own independence, objectivity, and professional skepticism.

In many cases, the service auditor and the user auditor are the same public accounting firm. The service auditor does not have full independence in scope as the external issuer auditor does; the service auditor's scope is determined by the client. But, imagine the difficulty of reporting a deficiency from a service auditor report performed by the same firm. Knowledge of whether a contracted service auditor accepted compensation for both audits or from another consulting engagement (such as PCI, internal audit, or penetration testing), can also be hard for the recipients of a service auditor report to know.

Rejecting a service auditor's report for any reason is very difficult because it greatly inconveniences the user entity who is paying the user auditor, causes additional cost to acknowledge a management vendor oversight issue, and creates greater expenses for the issuer auditor to complete adequate testing to offset reliance on a service auditors report. The difficulty in rejecting these flawed reports increases with each passing audit cycle where precedence is set for accepting flawed reports when a particular service organization is not rejected.

The "Why was this issue not raised last year?" management response to audit issues is a challenge that is hard to overcome without management, the issuer auditor, the service organization management, and the service auditor seeming incompetent or negligent in prior years. All parties are therefore discouraged from raising new issues on previously passed audit areas.

The second greatest point of failure is a lack of service organization audit committee and stakeholder accountability of the service auditor. Service organization management is generally free to select their scope and service auditor without influence from their audit committee or input from the audit

committees of their stakeholders. The lack of oversight has led to commoditization of the service auditor report industry. Management is incentivized to select the lowest cost provider with little concern of quality pushback. The quality of service auditing has eroded to the extent that I often observe that controls listed in service provider reports do not remotely resemble actual practice within the same service organizations I evaluate for IT security. Service auditors have no audit committee or board connections to reduce pressure to suppress findings. A qualified opinion by a service auditor is an open invitation to be replaced, especially as many services providers are smaller than their issuers, and less likely to have an independent board.

My recommendations are:

1) Make mandatory issuer auditor rotation effective after three years, and empower issuer audit committees to grant one year extensions provided the issuer's auditor meets PCAOB criteria for extensions.
2) Mandate that management provide all ICFR service auditor reports relied upon by the issuer firm to issuer audit committees to review the results and decide whether service and issuer auditors demonstrate independence, objectivity, and professional skepticism.
3) Review whether a service auditor with a client-directed scope, conflicts with the full scope independence of the external issuer auditor to obtain adequate supporting direct evidence. Imagine the difficulty of reporting a deficiency, when the same issuer audit firm produces an ICFR assertion service auditor report for the same company.
4) Issuer auditor audit committees should be responsible to enforce that issuer auditors be responsible for the timely completion of issuer auditor ICFR risk assessments, with substantiated submission of the accounts and actual ICFR objectives needed from a services provider auditor, justifying risks where an ICFR weaknesses originating from a service provider has been deemed to be potentially material and not able to be controlled by prudent issuer management monitoring and direct oversight controls.
    - The ICFR service auditor's audit deficiency evaluation should meet at least the same materiality thresholds and evidence quality criteria as predetermined by the PCAOB.
    - Require that the issuer's Chief Internal Audit Executive have open access to evaluate the external auditor's workpaper evidence adequacy on behalf of the audit committee to whom they also report, so that the audit committee's oversight can have a chance to be aware of inadequate testing to be more effective.
    - The PCAOB criteria for acceptable audit service auditor deficiencies would include at least the same areas it has found where special attention should be given for flagging a lack of independence, objectivity, and professional skepticism.
    - Determination of whether the audit committee grants an extension is performed during the third year of the three year rotation period on audit findings produced by the issuer's auditor in year two of the rotation period.
    - Each one year extension the issuer's auditor is granted should be based on the audit committee's evaluation of the previous year's audit findings to ensure time to transition

to a successor user auditor in the case where the audit committee does not grant an extension.

5) Consider the degree to which issuer audit committees reviewing service auditor reports also have a responsibility to support the review of service auditor independence to external issuer user organizations using the same ICFR report; including whether the same service auditor also received consulting compensation from the issuer or from sub-providers of the issuer.
6) Comment on whether it would be true that an issuer auditor would be required to obtain some direct evidence to test some ICFR service provider controls if a significant account with a high materiality risk of control failure, regardless of having a "perfect" services provider report. This may help drive home the ownership for opining on appropriately weighted risks and evidence.
7) Consider adding transparency of issuer-provided evidence request and collection status and issuer payment to the audit committee, and/or PCAOB, to reduce the ability for clients to influence the audit results by delaying the production of evidence to the last minute, and withholding a final report payment, which compresses reasonable evaluation time to perform due diligence and influences the reporting of quality issues due to a real business need to pay staff.
8) To expedite a focus on applying issuer industry quality improvements earlier, independently develop an issuer ICFR Auditing examination, pairing current expert PCAOB quality assurance knowledge with high control over the currency and quality of PCAOB issuer auditor educational expectations content, to ensure the greatest likelihood that correct and current PCAOB expectations are learned and knowledge of independence, objectivity, and skepticism specific to issuer ICFR needs is directly demonstrated by auditors.

User auditors who are confident in their ability to remain independent, objective, and professionally skeptical will have no problem producing quality evidence to support their case for annual extensions.

I would be pleased to further discuss my comments with you. The IT auditing and security testing industries are not immune to challenges, and are also examining how we can strengthen our quality control services. Should you have any questions in relation to this letter, please contact me at the number listed below.

Sincerely,

Jon Long, CISA, QSA
Senior Auditor at CompliancePoint
Industry Blogger at The Risk Assurance Guy
Phone: (404) 368-9228