From: Malcolm Schwartz [mailto:malcolm@crsassociatesllc.com]
Sent: Monday, February 26, 2007 3:31 PM
To: Comments
Subject: Comments on PCAOB Release 2006-007 of December 19, 2006

The basis for these comments includes my following experiences, as:

- One of the four principal contributors to Internal Control – Integrated Framework ("IC-IF"), issued in 1992 and which provided The COSO Framework used by many companies for complying with Sarbanes-Oxley ("SOX")
- One of the management consulting leaders at Coopers & Lybrand (later, PricewaterhouseCoopers) and in my current consultancy, in applying The COSO Framework from the time of its publication to date (review the web site of my current company for a complete list of my articles and speeches, www.crsassociatesllc.com)
- A member of -- and team leader of -- the recent COSO task force dealing with simplified guidelines for internal control over financial reporting ("ICFR") for smaller registrants
- A speaker and writer on the subjects of internal control and risk management, recently including:
  - A Financial Executives Research Foundation four-part series, titled "A Top-Down Approach to Risk Management & Internal Control," and dealing with:
    1. "Having a Business-Process Focus Tied to Business Planning," issued in May 2006
    2. "Using an Aggregated Risk Assessment to Reduce Documentation Costs," issued in August 2006
    3. "Using a Process Point of View to Reduce Documentation Costs," Issued in January 2007
    4. "Relying on Ongoing Monitoring to Test Controls Performance, to Reduce the Scope of Separate Testing," to be issued shortly

    This series uses case studies and a generic business template of processes and their component activities, as well as the activities' characteristics, to show how the costs of SOX compliance have been reduced by as much as a factor of five when this approach is followed
  - An article in the December 2006 issue of Strategic Finance, published by the Institute of Management Accountants, focusing on smaller companies and including a case study illustrating similar costs and benefits, and titled "Make Risk Management & Internal Control Work for You"
  - A January 18, 2007, program for the Institute of Management Accountants "Inside Talk Webinar Series," titled "SOX & Small Business: Less Is More," showing the above approach and using a case study, with the CFO of the study company participating.
- Having been a CFO of a corporation filing with the SEC (Booz, Allen & Hamilton), and a business unit controller, treasurer and CFO; and a group financial executive over a number of business units
- Having led consulting projects dealing with, among other matters, internal control and risk management, and business process and organization analysis and improvement, in financial management, general management and operations management, for clients in a number of industries.

Based on these experiences and my developed point of view, I believe that the proposed auditing standard is a major improvement. However, some further important improvements could make its impact clearer and greater.

These improvements would go further in clarifying that the proposed standard is for auditors, and not for managements; and that auditors should not expect managements to follow the proposed standard. As many have commented, Auditing Standard No. 2 ("AS2") became the de facto standard for many companies, who interpreted AS2 as providing the management approach in

the absence of guidelines for SOX compliance. Now, with guidelines being provided by the SEC concurrently with this PCAOB Release, it is clearer that the proposed standard is to shape how auditors are to audit. However, there is the risk that misinterpretation will continue, and incorrect inferences will be drawn, unless the PCAOB is quite explicit that: (1) this is a standard for auditors to perform audits, (2) the approach that managements take can be distinctive as long as the auditor is able to both perform the required audits and meet the proposed standard, and (3) companies that apply business process management ("BPM") or related techniques often embed internal control and risk management in their basic management and business processes, and derive ICFR as a byproduct.

This latter approach is deemed by many to be the most cost-effective way to enable ICFR. It integrates internal control and risk management into its management processes, thereby reducing the costs of developing and maintaining ICFR. It aggregates risk assessment – for a top-down perspective – from risk assessment built in to key activities. It begins with activity analysis, so that only activities whose inherent results are significantly uncertain need to be controlled (and this typically is the case for only 10% to 20% of the activities in any significant process). It integrates governance and management processes with business – or transaction – processes, so that costs are reduced by not having to maintain connectivity among checklists, process write-ups and other forms of documentation. It further integrates fraud detection into basic internal control and risk management, further reducing costs. It uses fully the principles of the COSO Framework. And it, as the COSO Framework recommends, relies on ongoing monitoring to confirm the performance of control activities, thereby reducing the costs of separate evaluations. Yet it could be inferred by an auditor, based on the PCAOB proposed standard, that this is not an acceptable way for management to enable ICFR. One reason for this incorrect inference is that BPM often identifies the activity components of each process, associates risk with the results of performing the activities, and then from this business template assesses top-down risk for the purposes of achieving its objectives (among which can be ICFR). When applied to ICFR, this approach derives the relationships to financial reports and disclosures, as opposed to beginning with them. Because the proposed standard states that a risk assessment begins with the financial statement accounts – as it should for the auditor – some auditors had not accepted the management approach as outlined in this paragraph, causing redundant and standalone approaches to use BPM on the one hand for sound business management, and to satisfy auditors on the other hand by separately building an audit-centric approach to compliance. In reality, having these separated approaches inherently adds risk, and cost, to a business. Further to support the position in this paragraph, recognizing that there are two approaches to risk assessment is consistent with the audit of financial statements, where business activities are performed to generate information used for financial reporting – financial reports are derived from business activities, in other words -- whereas audits begin with the derived financial reports.

Recognition of this approach also requires that BPM techniques and definitions be acceptable to, and generally understood by, auditors; so some wording in the proposed standard could be made clearer. Suggestions follow, for the Release itself and for the proposed standard, to avoid incorrect inferences, to not foreclose distinctive management approaches to ICFR, and to recognize that top-down risk-based assessments might not always begin with the financial statement accounts.

I. Introduction

Herein, it would help to avoid incorrect inferences by stating that: "…As described below, these proposals are designed primarily to …eliminate unnecessary audit procedures…"; and: "…simplify the audit requirements…"

II. Significant Changes to the Standard – would avoid incorrect inferences if it were changed to: "Significant Changes to the Auditing Standard"

II.A Focusing the Audit on the Matters Most Important to Internal Control -- would help to avoid incorrect inferences if it were to state that auditors use "…a top-down approach appropriate to auditing…"

- **II.A.1 Directing the Auditor's Attention Toward the Most Important Controls** – would help to avoid incorrect inferences if it were to state: "…by starting at the relevant top…" and later: "…to the significant activities in significant processes…"

II.B Eliminating Unnecessary (insert) **Audit Procedures** – would help to avoid incorrect inferences if it were to state that: "…the proposals would eliminate the requirement for the auditor to evaluate the process that management used…"

- **II.B.1 Removing the Requirement to Evaluate Management's Process –** would help to reinforce the compatibility of the audit approach with a management approach using BPM if it were to state that: "…Under the proposed standard, an auditor still would need to obtain an understanding of management process, such as a reliance on business process management as a means of establishing internal control and risk management of the activities of a business…"

- **II.B.2 Permitting Consideration of Knowledge Obtained During Previous Audits –** would further reinforce this compatibility by stating that: "…the risk factors described in the proposed standard and determining that an activity presents low risk overall (because, for example, the activity has low inherent risk and a low degree of complexity, or the activity has some risk that is mitigated by a following control activity, there were no changes to…"

- **…**

- **II.B.5 Recalibrating the Walkthrough Requirements –** would balance the discussion if it focused not only on transactions (and hence only business transaction process and their activities) but also on management and governance processes and their component activities, and if did not appear to restrict the tools supporting processes only to information systems, as follows: "…In performing a walkthrough, the auditor follows the selected governance, management or business process and its component activities from the information input to the originating activity and considers the activity flow and associated tools, such as policies and procedures, forms, and information systems, until the information output of the last activity is reflected, indirectly or directly, in the company's financial reports…" and "…the auditor must complete walkthroughs of all significant activities in significant processes…"

- **…**

- **II.D Simplifying the** (insert) **Audit Requirements**

- **…**

In regard to Appendix 1, the Auditing Standard itself, the following suggestions, by paragraph, are made, to avoid the incorrect inferences discussed earlier, and to reinforce the distinctiveness of and the compatibility between the auditor's approach and the approach that many managements might use to integrate ICFR with their basic internal control and risk management processes

- **5 –** would avoid incorrect inference by including a footnote to clarify that The COSO Framework is the framework itself, and not the accompanying illustrative evaluation tools (some auditors had interpreted that the evaluation tools are integral to the COSO Framework and had held clients responsible for applying those evaluation tools)

- **6** – would avoid incorrect inference by modifying the first bullet, as: "…knowledge of the company's internal control over financial reporting, which might be embedded in the company's management processes through its use of business process management tools, to integrate internal control over financial reporting with internal control over business operations…"

- **8** – would reinforce the compatibility of the two types of risk assessment, as: "…Risk assessment linked to the financial statements underlies the entire audit process described in this standard, and is compatible with the form of risk assessment used by many companies that links to their business processes and the component activities…"

- **16 –** would further reinforce this compatibility by stating that: "…A top-down approach for the auditor begins at the financial statement level (for management, a top-down approach might begin with the risks of uncertainty in the outputs of activity components of processes)…" and: "…and then works down to significant accounts and disclosures, relevant assertions, and significant activities in significant processes…"

- **18** – would further reinforce this compatibility if it stated that "…Company-level controls, at both the business unit and the corporate organization levels…"

- **20 –** would align with The COSO Framework, which is used rather widely, if the list of bullets included: "…whether, as a commitment to competence, there exists the knowledge and skills needed, and that these are specified…," and "…management's philosophy and operating style are consistent with sound internal controls and risk management…," and "…human resource policies and practices, and organization structure, are current, defined and communicated, and reinforce the control objectives of the company…"; and the bullet regarding misstatement would be modified to state that: "…pressures on management and employees…"

- **21 –** would avoid incorrect inference if the four bullets would begin with "…Activities…" instead of "…Processes…," and if the first bullet stated: "…to enter transaction totals into the general ledger or other consolidating device…"

- **22 –** would reinforce alignment with the management approach if the first bullet stated: "…Inputs to activities, including constraints and controls, tools and resources, and the work itself, the procedures performed, and outputs…" and in the fifth bullet: "…adjusting and consolidating entries, including standing and one-time entries…"

- **25 –** would avoid incorrect inference by stating that "…The risk factors the auditor should evaluate in identifying that significant accounts might be misstated include…";` and by expanding the listing to include the impacts of judgment, estimation, the potential of management override, the traceability of postings, the frequency of postings, the currency and completeness of related policies and procedures, and the timeliness of postings

- **28 –** would reinforce the compatibility of approaches if it stated that: "…and significant activities of significant processes, and also…"

- **32 –** would avoid incorrect inference if it stated that: "…Different types of major classes of transactions might result from activities that have different inherent risks associated with them…"

- **33 –** would avoid incorrect inference if it stated that: "…The controls over major classes of transactions exist within the company's significant activities in significant processes…"

- **34 –** would avoid incorrect inference if it stated that "…For each significant activity identified, the auditor should…" and "…understand its impact on major classes of transactions…" and "…Identify that it is an activity at which a misstatement…"; also, the last bullet does not deal with all frauds, but only those that could result in a material misstatement of the financial statements, so this could be further clarified and elaborated, to avoid audit work dealing with frauds that do not cause material misstatements.

- **37 –** would reinforce the compatibility with management approaches by stating that: "…the auditor has identified the activities in the process…" and, to reinforce the point about fraud discussed in paragraph 34, above, by stating that: "…the design of controls, including those related to the prevention or detection of fraud as described in paragraph 34…"

- **39 –** would further reinforce the above if it stated: "…At the activities at which important processing occurs, the auditor should question…"

- **43 --** would further reinforce the compatibility with management's approach by stating that: "…the auditor should recognize that control activities in governance and management processes vary in precision…" and "…some of these controls are designed to operate at the activity, process, transaction or application level…' and "…On the other hand, some of these control activities may be designed to operate…"

- **45 –** would further reinforce the above by beginning as: "…*Controls dealing with fraud and management override*…"

- **47 –** would avoid incorrect inference by beginning with a title stating: "…**Separately Evaluating Design Effectiveness**…" and stating that: "…The auditor should separately evaluate…"

- **48 –** would avoid incorrect inference by stating that: "…Procedures that the auditor performs to separately evaluate design effectiveness can include one or mix of inquiry of…"

- **49 –** would avoid incorrect inference by beginning with a title stating: "…**Separately Evaluating Operating Effectiveness**…"

- **50 –** would avoid incorrect inference, as well as align with the approach that some management use, by stating that: "…The procedures the auditor uses to separately evaluate operating effectiveness can include one or a mix of…walkthroughs, review of the results of ongoing monitoring (such as the recording of control performance using key control indicators, or KCIs, for such categories as accuracy, completeness, compliance and timeliness), and reperformance of the control

- **52 –** would align with management approaches by including as a bullet: "…The level of judgment and the related objectivity of the control activity

- **A13 –** would align with the above comments by changing the definition to: "…A **significant process** can be a business process that initiates, authorizes, processes and records a major class of transactions, or a management or governance process that provides the controls or constraints, or the tools or resources, to such a business process; and a **significant activity** is any specific step in such a process for which the output is sufficiently inherently uncertain as to cause significant risk of misstatement of financial results…"

If you deem it worthwhile, I will be happy to clarify or elaborate on these comments.

Sincerely,

R Malcolm Schwartz
Chief Operating Officer
CRS Associates LLC

office: 908-273-6967
cell: 908-803-8918
fax: 908-273-6226