February 27, 2007

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, business process and organization analysis and improvement, for clients in a number of industries.

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

These improvements would go further in clarifying that the proposed guidance is for management regarding its evaluation of ICFR, which can be embedded, as enabled by The COSO Framework, in a broader approach to risk management and internal control. With these guidelines being provided by the SEC concurrently with the PCAOB Release of a revised auditor standard, it should be clearer that that proposed standard is to shape how auditors are to audit, but not how managements are to manage. However, there is the risk that incorrect inferences will be drawn, as they have been in the past, and that auditors, and managements, will try to apply the audit standard as the management approach, unless the SEC is quite explicit that: (1) the approach that managements take can be distinctive from the audit standard as long as the approach can be audited, and (2) companies that apply business process management ("BPM") or related

techniques can 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 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 guidance is unclear about how a risk assessment begins, management might feel that they must begin with the financial statement accounts – as an auditor should – and some auditors might not accept 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 to a business.

Recognition of this approach also requires that BPM techniques and definitions be acceptable to, and understood by, all parties; so some wording in the proposed interpretive guidance could be made clearer. Suggestions follow, to avoid incorrect inferences, to not foreclose distinctive management approaches to ICFR, and to recognize that top-down risk-based assessments might not begin with the financial statement accounts from a management point of view.

I. Background

You note that “the methods of conducting evaluations of ICFR will, and should, vary from company to company and will depend on the circumstances of the company and the significance of the controls.” This being the case, then it is important for you not to omit approaches that will meet the requirements, because by omitting them you allow the inference that they are not acceptable approaches.

II. Introduction

- (Page 14) In providing reasonable assurance regarding the reliability of financial reporting, some registrants are confused about fraud: it is possible to be defrauded and to have reports be reliable. For example, a proper recording of the payment of a fraudulent vendor invoice properly reports the remaining cash, and is no more a misstatement of financial reporting than is the proper recording of a poorly executed sales promotion
- Page 14, Footnote 34 notes that IC-IF, in discussing the assessment tools provided in its third volume, cautions about their use. This should be stressed because In applying them I found them not to work, and had to modify them substantially, particularly for the components of risk assessment and monitoring

- **The two principles (Page 16) – evaluation by management of ICFR, and a risk-based assessment –**
- The notion that "…management may be able to use more efficient approaches to gathering evidence, such as self-assessments, in low-risk areas and perform more extensive testing in high-risk areas…" omits, and hence leaves unclear about acceptability of monitoring, particularly ongoing monitoring, as used in IC-IF; as a consequence, some have come to believe that the only form of assessment that is acceptable is separate evaluations

III. Proposed Interpretive Guidance

III.A. The Evaluation Process

III.A.1 Identifying Financial Reporting Risks and Controls

The concept of "entity-level controls" has misled people, and caused them to create and administer checklists that are separated from the work flows – the business processes. This in turn has led to added cost, as there becomes a need to integrate these separated evaluations, and in turn over time to maintain the integration. If so-called entity-level controls are treated simply as controls in other processes – that is, governance and management and business processes – and are integrated, then there is less cost to develop and maintain a system of controls. This being the case, and given the common usage of the phrase "entity-level controls," as well as not foreclosing this alternative design concept, of treating entity-level controls as the controls in management and governance processes, consider changing the wording to state "…the company's entity-level controls, or what some consider the controls in the company's governance and management processes…."

The statements about subsequent evaluations imply separate evaluations, and seem to ignore ongoing monitoring. If this inference is inappropriate, then it could be eliminated or mitigated if the following were added to the last paragraph: "…Alternatively, the evidence could be gathered from ongoing monitoring, thereby reducing substantially the need for separate evaluations…"

- III.A.1.a Identifying Financial Reporting Risks -- The identification of financial statement risks might begin with evaluating how the requirements of GAAP apply, but it then moves quickly to the integrity of transferring information to the general ledger and in turn to the financial statements. Yet this is omitted from the guidance being provided. The guidance could be strengthened by noting that financial statement risks also depend on activities as well as the application of GAAP, particularly the activities that enable the assembly of information into the financial statements and disclosures.

  Footnote 45 could more clearly state that there are two assessments (of the design of controls and of their operation). This could be emphasized by inserting the word "both," as "…involve assessing both the design and operation of controls…" Also, to clarify ongoing monitoring activities, the last sentence could be modified to state "…ongoing monitoring activities are often built into the normal recurring activities of an entity and include but are not limited to regular management and supervisory review activities..." This helps to stress process – or activity -- owner accountability, and such an owner might not be a supervisor or manager.

  Similarly, on page 23, consider inserting "…and their activities…" in the first sentence of the first paragraph, as follows: "…Management uses its knowledge and understanding of the business, its organization, operations and processes and their activities to consider…." In the same paragraph, fraudulent activity combines two distinctive ideas: the first deals with fraud that leads to poor financial reporting, and the second deals with fraud that does not affect financial reports but that leads to

poor control of assets. Nowhere in this guidance is poor asset control defined as corollary to poor financial reporting; so these two conditions should be separated, or the idea clarified.

- III.A.1.b Identifying Controls that Adequately Address Financial Reporting Risks -- Footnote 51 identifies a control as consisting of a specific set of policies, procedures and activities. It might be better to state that the design of a control is the design of such material, and the operation of a control is how that material is applied. Also, the wording allows for some confusion about function, activity and process. Better wording might be: "…The design of a control consists of a specific set of policies, procedures and activities put in place and operated to meet an objective. A control might exist within a specific function in an organization, or within a specific activity in a process…"

  In the first full paragraph on page 25, you state that "…It is not necessary to identify all controls that exist…" There are two clarifications that would be helpful. First, a company using control for purposes of operations performance often starts by identifying but not documenting all of its controls, and at the level of the activity components of its processes; and then it identifies those controls associated with risks that are important to achieving its objectives. If this is the case, then risk and control management is already in place, and the top-down assessment of risk and associated control for ICFR is a derived part of an embedded management process. Then, the better statement is that: "…It is not necessary to associate with ICFR all controls that exist…" Secondly, identifying controls is distinctive from documenting controls, but many companies and auditors are not making this distinction, and this is leading to the excessive amounts of documentation and cost; so, this might be better stated as: "…It is not necessary to document all of the controls that are identified…" In the same paragraph, one could argue that a control within a company's period-end reporting process is not an entity-level control, but that it is a control associated with a low-frequency recurring business process, and that it occurs at both the company/division/unit and at the corporate levels. This being the case, and so as not to have readers infer incorrectly that the example can only be considered as an entity-level control, it might be better to eliminate the parenthetical thought.

- III.A.1.c Consideration of Entity-Level Controls – This phrase has become common usage and should be retained, although it can be misleading. Perhaps wrong inferences could be reduced by changing the first sentence to read: "…Management considers controls on governance and management processes – often called entity-level controls – when identifying and assessing…" Later in this paragraph, it might be better to be consistent with this change and state that: "…Some of these controls are designed to operate at the process level, some are designed to operate at the activity level, some are designed to operate on the transactions that are enabled by specific activities, and some are designed to operate on the computer applications that enable the activities; and might adequately…"

  The second paragraph can lead to misleading inferences that control environment has little to do with ICFR. It might be better if this paragraph, and the example in it, dealt with whether such matters as tone at the top deal with specifically (rather than "…directly…") with financial statement amounts, and that the importance of these controls, and of control environment, might be balanced with specific controls relating to the accuracy of financial statement information.

- III.A.1.d Role of General Information Technology Controls – The first sentence allows the inference that IT-related controls are freestanding, as opposed to being parts of the activities and their risks in the process being addressed. This could be mitigated by ending the sentence with: "…exception report); and management might have

considered them as part of the tools and resources to be used in the activity as designed..."

- III.A.1.e Evidential Matter to Support the Assessment – This section supports that business-process management documentation is acceptable. Many companies use business-process documentation, and relate this to business-risk and internal control management. Using this sort of documentation for ICFR enables an integrated approach, which is more cost-effective than non-integrated approaches. Suggestions about the wording in other sections are simply to reinforce the wording of this section.

III.A.2 Evaluating Evidence of the Operating Effectiveness of ICFR

The second paragraph allows the inference that ongoing monitoring is an activity but not a control. It might be better to state that: "…Evidence about the effective operation of controls may be obtained from direct-testing of controls, and/or from ongoing monitoring…" And, later in the paragraph: "…should consider not only the quantity of evidence (e.g., sample size, or extent of ongoing monitoring) but also…" And, further in the paragraph: "…and, in the case of ongoing monitoring, the extent of confirmation through separate evaluations..." This simply uses, and reinforces, the approach described in IC-IF.

- III.A.2.a Determining the Evidence Needed to Support the Assessment – Reference to "…controls whose operation requires significant judgment…" might be better stated as "…controls whose operation allows significant judgment…"

  Later, this section notes that: "…When the controls are related to these financial reporting elements are subject to the risk of management override…, they should generally be assessed as having higher ICFR risk." This allows the inference that only a control is subject to management override, when often it is an activity that is subject to management override, and the control is designed to follow the activity so as to reduce the likelihood of management override. So, this might be better stated as: "…When the activities that enable these financial reporting elements are subject to the risk of management override, and the ensuing control to reduce that risk is not in place…, they should generally be assessed as having higher ICFR risk..."

- III.A.2.b Implementing Procedures to Evaluate Evidence of the Operation of ICFR – To stress the idea of ongoing monitoring as an appropriate solution, the first paragraph might state that: "…These ongoing monitoring procedures may be integrated with…"

  Later, the reference to "…direct tests of controls…" might be better stated as "…Separate evaluations of controls…," to be consistent with IC-IF.

  Also, Footnote 65 allows the inference that the use of what are called key control indicators (KCIs) is not acceptable as the basis of ongoing monitoring. KCIs came to be used with the application of IC-IF after its publication and before the enactment of SOX, and addressed the aspects of ICFR by measuring and reporting on accuracy, completeness, compliance and timeliness. As a consequence, KCIs also correlated with statements of assertion, and led to further integration of internal control and risk management, and hence to greater cost-effectiveness. It might be well to state in Footnote 65 that KCIs focused of ICFR are an acceptable way to provide evidence of the operation of ICFR

- **...**

III.A.3 Multiple Location Considerations

As discussed earlier, in III.A.2, this section allows the inference that risks are related to controls, and not to activities, when it is the control that mitigates the risk in an activity component of a process for those companies that use process management as a means of control. So, it might be better to replace the word "…control…" with the word "…activity…".

III.B. Reporting Considerations

III.B.1 Evaluation of Control Deficiencies

On page 43, to avoid the inference that an activity focus is not acceptable, it might be better to state that: "Management should evaluate how the activities and their controls interact with other activities and their controls when evaluating the likelihood that…"

…

Request for Comment

By providing the feedback, above, on the proposed interpretive guidance, there is no need for comments to the Commission's questions.

IV. Proposed Rule Amendments -- No suggestions are made for this section, and no responses are made to the "Request for Comment."

V. Paperwork Reduction Act -- No comments are made on this section

VI. Cost-Benefit Analysis

VI.A Background -- No comments are made on this section, except to support the capability to use of a management-focused approach as distinctive from an audit-focused approach.

VI.B Benefits

The proposed interpretive guidance addresses to some extent a more efficient and effective approach to ICFR. It does not explicitly address some further efficiencies, which the suggested changes earlier in this submittal would help to clarify and to prevent inferences that such approaches are not allowed.

VI.C Costs

As noted earlier, the BPM approach to supporting ICFR has been shown in case studies to reduce costs by as much as a factor of about five.

VI.D Request for Comment

It is difficult to comment on the costs and benefits of the proposed amendments, as they have only been available to apply and assess for a brief period. Furthermore, it is likely that few companies have defined their current compliance efforts in terms of work and cost segmentation that could be analyzed for "current" and "proposed" costs. However, if the proposals are meant to include the approaches addressed in the earlier comments – activity-level analysis of risks and control, derived from a generic business template, with integrated management, governance and business processes and their risks and controls – then there is evidence that such an approach can reduce the costs of compliance by as much as a factor of five, with no concomitant reduction in the level of control and the quality of reporting provided to investors. This evidence is contained in the case study in the article cited in the December 2006 issue of Strategic Finance; and in the ensuing webinar conducted by the IMA in January and available on the web site.

Also, there are studies that show that good control correlates with good performance, particularly when control derives from an integrated management approach
There are no unintended consequences associated with increased reliance on management judgment, as long as governance and management processes and their risks and controls are integrated with business processes and their risks and controls; otherwise, because one group is segregated from the other, there are risks due to lack of connectivity.

...

Please contact me if you need clarification on these comments.

Sincerely,

R Malcolm Schwartz
Chief Operating Officer
CRS Associates LLC