Comments to SEC on SOX – File Number S7-11-06

While I have some brief , but hopefully helpful, comments on many of the specific sections of the conceptual release, I wish to include a comment for “Section VI Solicitation of additional Comments” first. I wish to cover that first as I feel it is relevant to many of the problems mentioned in the prior sections.

VI Solicitation of additional comments:

It is my observation that a good portion of problems related to Managements assessment of internal controls is caused by an incomplete transition from a pre-SOX relationship with the external audit firm to a post-SOX relationship with their auditors.
Areas where this uncertainty about change in the relationship has had a major impact is in two areas.

1. A consistent understanding regarding the significance of a clean audit opinion on internal controls. I have noticed too many companies treating the audit as a “Pass or Fail” on SOX compliance in total, and , as a result, substituting the auditors opinion for a more thorough management review .
2. An effective use of control lists or of example procedures that may be provided from an outside auditor (E.G. the RACK from Deloitte, or the WCGW questions from E&Y). Companies do not always have the in-house expertise to incorporate this information into their internal control efforts.

1.) I believe that many companies are of the opinion that their auditor has the responsibility of determining and declaring their internal controls “Audited” , and thereby good and complete. Because of inherent limitations on the detail level of an audit, this may not be the case, however, this assumption is caused by not having anyone else available to tell them when they are compliant. I recommend a clear distinction of responsibility be disseminated for Auditing vs. Compliance determination. My interpretation is that by auditing a companies management assessment of internal controls, the external auditor has fulfilled their legal responsibility, but that this in no way absolves or shields management from their responsibility to design, implement, document, and review their internal controls to their own level of detail knowledge and professionalism.
Unless it is intended by the law, management should not assume that audits are their measure of success or the final measure of compliance with SOX internal control requirements.

2.) Samples that may be provided by external audit firms of control objectives, activities, and risks (WCGW) are comprehensive and require a consultant or professional auditor to make effective use of. Companies who inadvertently misuse samples or control matrixes that they may acquire from an audit firm **will end up with precisely all the problems related to excess controls and costs that have been mentioned over and over by issuers**.

The only way to understand the depth of this problem is get a copy of the controls from all of the big 5 audit firms and try to organize them to comply with the recommendations of a “Top Down” internal control design process.

Page 13 Question #1: I believe additional guidance for companies will be helpful to all issuers, however the guidance must, in some way, address the difference in detail and conceptual granularity desired by the external auditors as contrasted to the companies management. See above Section VI comments.

Page 14 Question #2: Additional guidance must address the conflict in the details required by auditors vs. Management – even if two versions of documentation are needed.

Page 14 Question #3: Additional topics must clearly and simply define what authority (if any) the external auditor has in determining when Management is “Done”, and has succeeded with its internal control program.

Page 15 Question #10: To me this is the most important issue for success in internal controls for SOX compliance. See all of the above.
A possible alternative solution is for the SEC’s enforcement division to staff up with specialists to provide a brief review of a companies internal controls, and provide authoritative guidance on compliance or non-compliance with FCPA and SOX.

<u>Section III Risk and Control Identification:</u>

Questions 11 through 18: There are way too many controls organized in too many different ways. I believe this is caused by companies looking at the total universe of possible controls their audit firm may audit, and then applying these controls in an unorganized manner without “process context”.

<u>Section IV Managements Evaluation:</u>

Questions 19 through 23: Most of the problems in this area are created by applying controls (both entity level and activity level) without being able to organize the controls into a hierarchy, or put them in context with a process flow chart that would allow justification of the minimum number of controls required to test the effectiveness of the total process – not small pieces of the process.

Questions 28 through 30: IT controls should be broken out as a separate issue and should be designed by an IT specialists for the source transaction database and security – as well as change management. Transaction flow charts must be developed from an application viewpoint and conversion points or other risk points controlled. This will allow the minimum number of required controls to be determined.

Section V Documentation to support the assessment:

Question 31: The initial documentation was excessive and costly because companies tried to use unorganized controls provided by their auditors or other sources without the context of a good process flow chart, and a logical, documented selection of what controls were needed for their specific company to provide effective internal control over specific risk attributes; they tried to do too much and the documentation reflected that.

Question 32 through 35: I believe that “rough cut” documentation should be developed and used during the project to design and test controls (especially for smaller companies). Then specific documentation for management, Accounting auditors, and IT auditors should be created by technical writers from the rough documents.