Comment Letter S7-11-06
Framework for Top-Down Risk Assessment

July 25, 2006

Nancy M. Morris, Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Re: File Number S7-11-06

Dear Ms. Morris:

I appreciate the opportunity to provide my perspective to the Securities and Exchange Commission ("SEC") regarding Concept Release 34-54122. As a Sarbanes-Oxley (SOX) compliance practitioner and professional internal auditor, I believe guidance regarding the top-down, risk-based assessment is an excellent opportunity for the SEC to help focus the efforts of management in the SOX arena. Utilizing an effective, risk-based approach will help ensure compliance efforts efficiently meet both the spirit and letter of the law.

This comment letter presents a framework for implementing a top-down risk assessment, which the SEC may consider helpful as it considers related guidance. The framework identifies five primary levels of assessment that are generic to any company. Various processes can be placed into one of the five levels, providing a basis for determining which controls to include in the scope of the assessment (i.e., "control rationalization.")

Risk Assessment Framework Summary

The five levels are described below:

1) Level One: Company-level Controls: Each company should generally focus top-down, meaning first considering company-level controls specified in the Control Environment, Risk Assessment, Information and Communication, Monitoring, and Control Activities components of the COSO Framework. The strength of these company-level controls is considered in determining the testing effort at all subsequent levels. Company-level controls should be assessed broadly and in-depth, with coverage of a significant majority of the "Points of Focus" within the COSO Framework. The "tone at the top" and implications of the incentive structure on financial reporting should be key focus areas. Only a limited scope reduction in the number of company-level controls tested relative to "Year 2" levels would be appropriate.

2) Level Two: Core Accounting Processes: These processes include the monthly closing and external reporting processes. Typical activities included in these processes involve journal entry preparation, account reconciliation, disclosure preparation and financial statement review. Related controls are generally performed by accounting department personnel and represent the final control points for all of

the financial processes of the typical organization. These controls would be tested each year and would not be authorized for multi-year rotation. Only a limited scope reduction in the number of Core Accounting controls tested relative to "Year 2" would be appropriate. Historical results of related testing would bear on the control rationalization decisions for subsequent levels described below.

3) Level Three: Revenue Processes: The "order to cash" processes, including order receipt, credit acceptance, order processing, shipment, billing, collection, etc. are the most significant of the transactional-level processes from a SOX perspective, because the majority of significant accounting frauds and restatements have historically been revenue-related. Only a limited scope reduction in the number of revenue controls tested relative to "Year 2" levels would be appropriate. Revenue-related controls would not be authorized for multi-year rotation.

4) Level Four: Transactional Processes: The remaining processes that generate accounting information include processes such as accounts payable, payroll, treasury, inventory, tax, capital assets, etc. A first layer of transactional controls within these processes is generally supported by a second or third layer of controls performed in the "Core Accounting Processes" (Level 2 above). While these transactional processes have certain complexities, they generally involve a high-volume of activity handled in a consistent manner and are unlikely to be involved in significant restatements or frauds. Further, they typically involve particularly robust controls such as inventory counts or bank reconciliations, which provide a very high level of assurance. As such, a moderate to aggressive control rationalization is merited. This supports a 25% to 50% reduction from the number of controls evaluated during "Year 2." Variation in the extent of rationalization would be expected across the transactional processes, based on the relative risk of each process based on various risk factors already in the guidance. Further, certain transactional controls could be subject to multi-year rotation. A formal risk assessment of each of the company's transactional processes would be required to support management's control rationalization and rotation decisions.

5) Level Five: IT General Controls: The indirect relationship of these controls to financial statement accuracy, combined with few incidents of contributing to significant financial restatements or fraud, support a very aggressive control rationalization to the point of nearly eliminating this area from the assessment. This implies a 75% or greater reduction in the number of these controls evaluated relative to "Year 2." Further supporting this view is the understanding that key application-level controls are considered along with the specific transactional processes described above. Two key areas would remain: An evaluation of "change management" controls applied to specific, critical financial systems changes (if applicable); and security access to key financial data and programs. Beyond these, most of the other IT general controls should be removed from the scope unless a particular condition specific to the company merits inclusion. The SOX community would benefit from a specific (and short) list of control objectives to dramatically reduce effort in this area.

These five levels and corresponding control rationalization approaches are summarized in Table 1 at the conclusion of this document.

Summary - Impact of Framework Risk Level on Assessment

The first two risk framework levels (Company Level and Core Accounting Level) represent the "bull's-eye" of compliance. They are the foundation of the control structure of the company and their relative strength or weakness is critical to determining the breadth and depth of SOX assessment necessary to meet the "reasonable assurance" threshold of the standard. Rigorous testing of the controls in the first two levels should occur every year as part of the SOX 404 assessment. The assessment of these levels would be expected to be both broad and deep in terms of number of controls evaluated and nature of evidence obtained through testing. Current year and historical results of the assessment for these first two levels impact the nature, extent, and timing of testing of the remaining levels. The impact on the control rationalization decisions of other processes should be documented by the company.

Controls within the remaining assessment levels would be subject to increasingly aggressive "control rationalization" (i.e. reduction in number of controls tested to focus on the most important controls in each process). Multi-year rotation would be considered for controls in transactional processes (Level Four), which presently form the bulk of the assessment efforts even though these are generally lower-risk processes.

Conclusion

A top-down, risk assessment framework for supporting control rationalization would be a very helpful addition to the SOX guidance. SOX efforts based upon current interpretations of PCAOB Auditing Standard Number Two result in an assessment that is comprehensive but not sufficiently risk-based, resulting in costs that may exceed the benefits for most companies. The SEC can help bring the cost-benefit of this standard into better balance with specific guidance regarding top-down risk assessment. A substantial "return on investment" will be obtained by encouraging aggressive control rationalization for the basic transactional processes, while simultaneously minimizing the impact on the level of assurance provided.

Table 1
Control Rationalization Matrix
By Risk Level

Framework Risk Level	Impact on Assessment of Lower Risk Levels	Control Rationalization vs. "Year 2"	Recommended Control Reduction vs. Year 2 Level	Controls Eligible for Multi-Year Rotation?
1. Company	Yes	Minimal/None	<10%	No
2. Core Accounting	Yes	Minimal/None	<10%	No
3. Revenue	No	Limited	10-25%	No
4. Transactional	No	Moderate to Aggressive	25-50%	Yes
5. IT General Controls	No	Very Aggressive	75%+	No