

February 15, 2007

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

RE: SEC FILE NUMBER S7-24-06

Dear Secretary:

The SEC has recognized that the proposed amendments to the SOX assessment rules may introduce new competition from software vendors in the supply of services and products to assist managers of public companies in their evaluations of ICFR, and has invited comments from vendors on that subject.

Our comments and suggestions for change that would, in our view, increase competition and improve the ability of software vendors to more effectively add value and to assist managers in their evaluations of ICFR are attached.

Paisley is a leading provider of software for governance, risk and compliance. With more than 500 successful deployments, our proven Sarbanes-Oxley solutions dramatically reduce the time and cost required for management to document their evaluation of ICFR. With more than 11 years of expertise in governance, risk, and compliance (GRC) solutions and the largest installed base of any GRC solution vendor, Paisley has the demonstrated track record to meet Sarbanes-Oxley compliance needs.

Paisley believes the following three principles are essential for regulations to foster competition and improve the ability of software vendors to more effectively assist managers in their evaluation of ICFR. The regulations should:

1. Balance the quantity and quality of information required on risk and control and balance the use of Top-down vs. Bottom-up approaches in assessing ICFR effectiveness.
2. Improve the reliability of financial processes by including process performance as an element of ICFR.
3. Integrate ICFR with management's overall Governance, Risk and Compliance (GRC) activities.

These principles are consistent with and supportive of sound cost effective regulation.

Regulation that achieves its goals while adding value to business is the key to promoting growth and competitiveness among software vendors and improving the software products available.

Rules that approach ICFR evaluation and reporting as another costly "silo-based" assurance activity will limit, not support, the growth of value-adding technology and resulting competition in this industry. ICFR audit standards should be based on regulations that reflect these principles.

1. Balance the Quantity and Quality of Information Required on Risk and Control and Balance the use of Top-Down vs. Bottom-Up Approaches

Better Balance Risk and Control Information

Achieving a better balance of risk vs. control information will drive up the quality and quantity of information available to assess the reliability of ICFR and lead to better financial disclosure.

The amendment as proposed remains strongly anchored in a control-based approach.

A balanced approach would provide guidance to support far more extensive risk identification and risk assessment, including the identification and categorization of specific current and historic risks to financial reporting in each company, industry and disclosure, their root causes, indicators of their likelihood and significance and would support tracking details of incidents where risk events have occurred.

In short, the quality and quantity of information gathered and analyzed regarding risk and its attributes and characteristics should be balanced with that now gathered and analyzed on controls.

Balancing the proposed guidance to include more information about risk and the attributes of risk will reduce SOX implementation cost by focusing management and auditor attention on specific risks known to cause financial reporting errors and on the most cost effective controls proven to be effective in their mitigation.

One way to quickly tell if an approach is risk-based vs. control-based is to assess the relative emphasis placed on risks vs. controls.

Figure 1 below assesses the degree to which an approach is control or risk-based.

The right hand column indicates the Risk to Control ratio. In other words, the simplistic ratio indicates whether a particular framework is risk or control-based by calculating the proportional references to risk vs. control in its text. In this case, for example, the proposed new guidance, with a ratio of 1:3.3, refers to controls approximately 3.3 times more than to risks. A balanced approach would have a 1:1 ratio. The Basel II framework is a risk-based approach with a risk to control ratio of over 12:1. A risk to control ratio of this magnitude is not unusual outside the literature and standards of the auditing and accounting professions. It represents a fundamentally different but at least equally valid perspective, on how risk can be understood, predicted and managed.

Simply put, the risk to control ratios for both the new PCAOB standard and the SEC interpretive guidance suggest that both documents are decidedly control-based, driven from an audit perspective and not a management perspective, and are emphatically neither risk-

based nor balanced. Both seek to emphasize and give more weight to the identification and assessment of controls. Better balance is required.

A close reading of both documents suggests that not only are controls emphasized more than risks, but that more attribute information is gathered about controls than about risks. For example, inherent risk, residual risk, risk indicators, risk cause, risk models and risk tables are not mentioned or considered in the proposed amendment. These and other risk attributes are the currency of true risk-based approaches. On the other hand, the SEC guidance seeks to gather such attributes of control as preventive, detective, operating effectiveness etc.

Figure 1			
Assessing the approaches – are they risk or control-based?			
	Risk Count	Control Count	Risk to Control Ratio
Proposed new PCAOB standard PCAOB Release No. 2006-007 December 19, 2006	108	590	1:5.5
SEC Interpretive Guidance Dec 20, 2006	137	417	1:3.3
Included for comparison only: July 2004 Final Release Basel Committee on Banking Supervision (International standards for a risk-based approach to capital measurement in financial institutions)	1609	136	12:1

Software tools are capable of analyzing risk, enabling root cause of failure analysis and scenario analysis and clearly linking the relationship of risk information with controls. Guidance that balances risk analysis with appropriate information on controls would drive down compliance and audit costs for business, better use the value adding capability of software and produce more reliable financial disclosure.

More Focus on the Top

Increasing the emphasis on top-down approaches and the involvement of management and staff in the assessments will drive down long term cost and increase sustainability.

Increased top-down assessments will drive down management certification costs, enhance accountability, identify problems earlier and lead to more resilient solutions to ICFR issues.

Management can focus on company level assessments and manage ICFR strategically no differently than other strategic business issue.

The proposed amendment does not go far enough toward balancing a top-down with a bottom-up approach. It fails to require management to gather sufficient information and draw appropriate conclusions from company level information.

Figure 2 below illustrates a framework for assessing top-down vs. bottom-up approaches. We believe the SEC guidance has strong elements of high Q3/low Q2 characteristics.

True top-down approaches would seek to form more and stronger conclusions on the overall health of the organization from entity level information. The inability to do so should be considered a deficiency in itself. Entity level assessments would focus on risk and vulnerability but would also focus on company level controls and culture, specifically on Control Environment, Monitoring and Risk Assessment. We believe more balance is required.

Figure 2 Characteristics of Top-Down vs. Bottom-Up Risk and Control Frameworks >>>Shifting from Risk Mitigation to Business Improvement>>>		
>>>Shifting from Bottom-Up to Top-down orientation >>>	Q2 – Top-Down Control-Based Characteristics <ul style="list-style-type: none"> • Focused on control identification and assessment at the organization entity level • Significantly more controls than risks are identified and described. (risk:control ratio of 1:3 or greater) • Significantly more emphasis on describing important attributes of control (preventive, detective, operating and design effectiveness, automated, manual, primary, secondary etc.) • Internal audit provides assurance on reliability of management control effectiveness assessments. 	Q1 – Top-Down Risk-Based Characteristics <ul style="list-style-type: none"> • Focused on identifying and assessing plausible entity-level risks. • Typically identifies more risks than controls. (risk:control ratio of 3:1 or greater) • Significantly more emphasis on identifying important attributes of risk. (E.g. source, category, inherent, residual and target significance and likelihood; risk indicators, residual risk status, root cause of failure etc). • Management is accountable for directing work unit assessments of risk and control. • Internal audit provides assurance on reliability of risk and control assessment processes.

Figure 2 Characteristics of Top-Down vs. Bottom-Up Risk and Control Frameworks >>>Shifting from Risk Mitigation to Business Improvement>>>	
Q3 – Bottom-Up Control-Based Characteristics <ul style="list-style-type: none"> • Focused on control identification at the process, system or transaction level. • Gathers extensive information on attributes of controls (preventive, detective, operating and design effectiveness, automated, manual, primary, secondary etc.) • Identifies far more controls than risks (ratio of 5:1 or greater) 	Q4 – Bottom-Up Risk-Based Characteristics <ul style="list-style-type: none"> • Focused on risk, incident and cause of failure identification at the process, project or system level. • Typically identifies far more risks than controls. (ratio of 5:1 or greater) • Significant emphasis on identifying all attributes of risk. (E.g. inherent, residual and target significance and likelihood; risk indicators, residual risk status, root cause of failure etc). • Work groups are accountable for assessing and reporting on risk and control.

The root causes of most material SOX deficiencies are discernable at the entity level. More assessment work and stronger conclusions should be required and reported at that level. GRC software is capable of providing senior managers with aggregated knowledge about risk and the reliability of controls at every level of the organization.

Far more guidance is necessary on how to assess, grade, report and remediate the conclusions that flow from an entity level assessment.

In addition, we believe that shifting more direct accountability for risk and control assessments to work groups supported by quality reviews by internal audit will enhance accountability and improve the quality of information available for ICFR assessment by management. Reliable work group information on risk and control aggregated for management analysis and is essential for reliance on entity level controls. GRC software can support this shift.

2. Promote Improvement of Financial Processes

Regulations requiring measurement and improvement of financial processes will provide tangible benefits for SOX compliance and link to other GRC initiatives.

SOX compliance should result in and must not impede business process performance improvement. Good SOX regulations and related audit standards must recognize strong, reliable financial process performance rather than merely reporting control deficiencies. Whatever the other merits of SOX, business will also expect economic benefit. In fact, the huge net cost of SOX compliance is the largest single criticism business has expressed. Without a linkage to improved financial and other process performance, SOX will not be sustained or sustained only grudgingly and at great expense. SOX regulations and software must embrace and support improved financial process performance reporting and the use of business process improvement tools in order to add value.

The proposed amendment would be far stronger if it required management analysis and reporting of business process performance in reaching a conclusion on ICFR. A focus on the performance of financial processes would include guidance on setting performance indicators, process performance measurement, event and incident tracking and process benchmarking within an enterprise and across industry groups. Tools and software already exist to support business process monitoring and business process improvement. Software will add tremendous business value in supporting process analysis and process improvement.

3. Recognize and Promote the Integration of Governance, Risk and Compliance (GRC)

Regulation that recognizes the comprehensive, integrated nature of corporate governance, risk and compliance will produce more reliable, consistent information and be of significant value to all corporate stakeholders.

Our clients are seeking to better manage all of their governance risk and compliance needs. To do so efficiently and effectively they must integrate, manage and audit a wide range of regulatory, internal policy and other requirements.

Over the long haul, integration of GRC, including SOX, must involve collaborative and interactive participation of management, specialists, auditors and work teams to produce rich, detailed, reliable information on ICFR and other GRC issues. ICFR assessment tools and technology must support work flow and collaboration across the organization and from its highest reaches to its front lines and it must be compatible with the goals of integrated GRC.

GRC knowledge must be created by and be accessible to managers, professionals and auditors throughout the organization and it must integrate with other assurance information developed in the organization. The quantity and quality of GRC information must improve and the participation by work teams in the SOX process must increase.

Figure 3 below describes 4 quadrants differentiated by the quantity and quality of GRC information and the extent of participation and ownership of management and work teams vs. specialists such as auditors.

Over the years, business around the world has made substantial progress in improving quality, safety and environmental compliance by shifting towards a Q1 approach by shifting accountability to work groups to as large a degree as possible.

To a large degree SOX regulations surrounding ICFR certification and audit have been approached from a Q3 perspective.

The role of internal and external audit is critical in a Q1 approach. Their role is to quality assure management's assurance data and to report on the reliability of management's assessment processes. This is a far more sophisticated and demanding role than now played by most internal or external audit groups but completely consistent with the intended role of a professional internal audit organization in an integrated GRC environment.

Integration of GRC supported by software will enable a shift toward a Q1 approach. Regulatory frameworks must support or at least not prevent that shift. We believe the SEC guidance reflects Q3/Q2 characteristics.

Figure 3		
Increasing GRC participation of management vs. specialists »»»»»		
Increasing quality and quantity of reliable GRC information»»»»»	Q2 – Proactive Specialist driven assurance reporting <ul style="list-style-type: none"> • Audit or other specialists create reliable assurance data for the business. • Focus on residual risk assessment across the entity. • Risk acceptance decisions made by managers and work teams. 	Q1 – Proactive Management driven assurance <ul style="list-style-type: none"> • Work teams create and own residual risk data. • Work team data is quality assured by internal auditors or other specialists. • Audit reports on the reliability of management processes.
	Q3 – Reactive Specialist driven effectiveness reporting <ul style="list-style-type: none"> • Auditor or specialists creates assurance data to support its opinions. • Deficiencies and exceptions are subjective. 	Q4 – Reactive Management exception certification <ul style="list-style-type: none"> • Management certifies processes as required. • Deficiencies and exceptions are defined for management.

The proposed amendment will hinder the GRC movement to the extent it embraces tools, definitions, concepts and methodologies that isolate ICFR assessment information in a silo created by and meaningful only to specialist users. Doing so inevitably shifts accountability for risk acceptance and control design decisions to those experts and away from management and work groups.

Achieving and sustaining benefits of integrated GRC require the active, knowledgeable participation of management and professional staff across the organization supported by internal audit in a quality assurance role.

The proposed amendments should clearly recognize and reward, and must not penalize, the use of accepted globally recognized standards and terminology for identifying risk and controls as they relate ICFR and must provide guidance on assessing and reporting ICFR effectiveness that is clear, practical and unambiguous to operating managers and professionals.

To do so they must recognize proven tools and the best practices of management in all GRC assurance professions, rather than embody practices, concepts and tools unique to the accounting and auditing worlds.

The proposed amendment should be broad and flexible enough to be understood and used for the collection and assessment of reliable information on risk and control for a variety of purposes and should reflect the input of risk and control experts in other areas of GRC.

Yours truly,



Bruce W. McCuaig
 Chief Risk Officer and Principal Consultant
 bruce.mccuaig@paisley.com