Tim Leech, FCA, CIA, CCSA, CFE
Chief Methodology Officer, Paisley Consulting
and
Parveen P. Gupta, LLB, Ph.D.
Magee Distinguished Professor of Accounting, Lehigh University

April 1, 2005

Jonathan G. Katz, Secretary
Securities and Exchange Commission
450 Fifth Street, NW
Washington, DC 20549-0609

Reference: File Number 4-497 re Experiences with Implementing and Evaluating Section 404 of the Sarbanes-Oxley Act of 2002.

Dear Mr. Katz:

We respectfully submit this letter in response to Commission's call for written comments seeking feedback from Registrants, accounting firms and others in implementing the new internal control over financial reporting requirements under Section 404 of the Sarbanes-Oxley Act of 2002 (the Act). This letter reflects our personal views and not those of our respective employers.

Since the passage of the Act in 2002 we have closely followed developments in this area and worked with hundreds of clients around the world that must comply with these new requirements. We have developed a broad range of technical training workshops and e-learning modules that cover the legislation, SEC Final Rules and PCAOB Auditing Standard No. 2 (Auditing Standard No. 2). We are involved in conducting various research studies that focus on understanding the "value relevance" of control deficiency disclosures including the reaction of the markets to these disclosures. As a result of our research we have reviewed and analyzed all control deficiency disclosures that have been filed by Registrants with the Commission during 2004. As authors of this paper we have more than 40 years of work and research experience in the areas on external and internal auditing, and risk and control assessments.

Our reading of the various speeches delivered by numerous SEC and PCAOB officials, and numerous articles and commentaries published by the business press tells us that the Commission and the PCAOB face enormous political pressure to "water-down" or even negate some of the requirements imposed by Sections 302 and 404. While we believe that there are a number of areas of the regulation that require changes to make the rules more practical and cost-effective, we strongly believe that the Sarbanes-Oxley Act of 2002, especially Sections 302 and 404, were necessary and appropriate and their implementation has significantly improved the reliability and usefulness of the accounting disclosures of U.S. Registrants. It appears that for the first time on a global scale C-suite executives and boards of directors are taking a hard look at their company's corporate financial reporting practices and disclosures.

We hope the Commission and the PCAOB will consider our comments as they deliberate on their course of action going forward. To fully appreciate the importance of Sections 302 and 404 it is first important to briefly revisit the history related to the Act.

1. Brief Historical Perspective

The notion of requiring management to rigorously assess the adequacy and effectiveness of controls over accounting disclosure and report major control deficiencies to the auditors and investors is far from new. It is essentially the same information that was called for in **1978** by the Commission on Auditor's Responsibilities, better known as the Cohen Commission. In the *Summary of Conclusions and Recommendations*, this blue ribbon commission convened by the American Institute of Certified Public Accountants (AICPA) states that

> "Users of financial information have a legitimate interest in the condition of the controls over the accounting system and management's response to the suggestions of the auditor for correction of weaknesses. Those matters should be disclosed in the proposed report by management. It is consistent with the normal responsibilities for financial reporting that primary reporting responsibility be assigned to management, with a report by the auditor on management's representations. The auditor should report on whether he agrees with management's description of the company's controls and should describe material uncorrected weaknesses not disclosed in that report."[1]

Although the Cohen Commission correctly identified real shortcomings in the way financial statement audits were being conducted in the 1970s, unfortunately the auditing profession chose not to address the issues at that time. The recent frauds by companies like Enron and WorldCom finally provoked Congress which, by rapidly enacting Sarbanes-Oxley Act of 2002, has now put into motion some of the very same key changes to the audit process and management reporting that the Cohen Commission prophetically called for over 25 years ago.

Describing the primary responsibilities that Sections 302 and 404 assign is relatively easy. Management of a company should identify risks that threaten the reliability of the assertions or claims implicit in their financial statements and note disclosures; identify, document, and assess the design and operating effectiveness of the controls in place to mitigate those risks; and conclude whether the existing controls constitute an "effective" system of internal controls over financial reporting. Serious deficiencies in internal controls, including what the SEC and PCAOB regulations call "significant control deficiencies" and "material control weaknesses" must be disclosed to the company's external auditors and the audit committee. Material control weaknesses must also be reported to the SEC by the Registrant in its periodic filings. Under the current rules, the existence of even one material control weakness precludes management from concluding that it has an effective system of internal control over financial reporting in place. The company's external auditor is charged with reporting on whether they agree with the conclusions reached by management and whether, in their opinion, the Registrant has an effective system of internal control over financial reporting in accordance with an established control framework.

The key problem with the current regulations isn't that formally and rigorously assessing and reporting on internal controls over financial disclosures doesn't make sense. What is problematic is the way these regulations have been interpreted and implemented in practice.

[1] AICPA, The Commission on Auditors Responsibilities: Report, Conclusions and Recommendations, (AICPA: New York), 1978, p. xxiii.

2. Underlying Problems

Based on the comments filed with the Commission to date the Registrants would appear to have two major complaints related to Sections 302 and 404 of the Act: excessive and unnecessary expense and widespread confusion. The most recent FEI survey dated March 21, 2005 estimates $4.36 million as the average cost of compliance for companies with average revenues of about $5 billion.[2] We believe these complaints are fully justified and should be addressed. In our opinion, the complaints about expense and confusion are symptomatic of a number of serious underlying problems that are discussed below:

2.1 Presumption that a Binary Conclusion on the Effectiveness of a Registrants' System of Internal Control over Financial Reporting can be Objectively Reached and is Useful

In our opinion, a major area for debate in the current regulations is the presumption that the management, as well as the company's external auditors, can objectively arrive at a binary/pass/fail conclusion about the effectiveness of a Registrant's system of internal controls over financial reporting (i.e. is or is not "effective"). Given the current state of guidance, methodologies, and tools, we do not believe that it is possible to unequivocally conclude, on a consistently repeatable basis, that a Registrant has, or does not have, an "effective" system of internal controls over its financial reporting. Concluding whether a Registrant has, or does not have, an effective system of internal control over financial reporting is like concluding whether a Registrant has passed or failed a prescribed test. If the criteria for assessing the effectiveness of internal controls over financial reporting was so "objective", and the methodology to conduct such assessments had the characteristics of "representational faithfulness" (that we are still trying so hard to achieve in accounting measurements), we would accept the validity of such pass/fail conclusions on a Registrants system of internal controls over financial reporting. Unfortunately, this is not the case. For example, the Malcolm Baldrige quality examiners, rather than making a binary determination about the likely "effectiveness" of quality programs at a company, assign a score on a number of dimensions that are designed to indicate the presence or absence of a reliable quality system. These scores are then used to determine, in a somewhat objective fashion, the degree to which a company currently employs a high performing quality system. Such an assessment clearly tells the company in which areas it scored low and what it could do to improve. If a similar assessment model is implemented for assessing and reporting on a Registrant's system of internal control over financial reporting many of the current problems could be alleviated.

2.2 Absence of Guidance for Managements on Control Assessment Criteria

The current regulations require management and external auditors to arrive at the binary decision of whether a Registrant has or does not have an effective system of internal controls over financial reporting. This is the primary driver of higher costs and confusion in the absence of practical and generally accepted control assessment criteria that company managements can use to assess and report on the effectiveness of their systems of internal control over financial reporting. Simply put, Registrants and external auditors are struggling with how the control assessments must be done and reported on a consistent and a reliable basis. The Commission and the PCAOB require that management and auditors assess a company's system of internal controls over financial reporting against an acceptable control model. Both the SEC and PCAOB reference COSO 1992 as an acceptable framework to guide this work. We recognize that COSO

[2] FEI Special Survey on Sarbanes-Oxley Section 404 Implementation, March 2005, Executive Summary.

was a significant positive step in 1992 but it was never designed to serve as a benchmark for company managements to assess and report on the efficacy of their internal controls over financial reporting for the very reasons mentioned in the earlier comment.

Although COSO 1992 is the dominant control model for reporting recommended by the SEC and the PCAOB, we are very sceptical that it can be used to produce "reasonably consistent qualitative and quantitative measurements of a company's internal control" over time. Our experience in the areas of risk and control assessments with hundreds of companies indicates that prior to SOX very few internal auditors provided senior management and audit committees with reports on how their organizations size-up against the COSO criteria. Similarly, very few external auditors wrote management letters that made explicit reference to the five COSO categories and how their audit clients stacked-up against the COSO criteria. We believe it can be empirically proven that similarly trained management and/or auditors will not consistently reach the same conclusion about the effectiveness of a Registrant's internal control system relative to the COSO framework when independently presented with the same set of corporate facts or circumstances. Some of the comments in the NASDAQ March 2, 2005 survey confirms this belief:

- No consistent approach from the audit firms-each had different definitions and process models for attestation.
- What constitutes final attestation of the process? Scope of work seems never ending.
- Since the Big 4 didn't have agreement on a clear standard, no cohesion among them resulted and they tried to "out do" each other to be safe.

2.3 Power Imbalance

The absence of practical guidance for Registrants on generally accepted control assessment criteria has contributed to a significant power imbalance between the management and their external auditor. It is the next most contributing factor for the current level of dissatisfaction and high costs associated with complying with Section 404.

Under the current requirements, the management of a company is required to grade its internal control weaknesses using a three tier system – control deficiencies, significant control deficiencies, and material control weaknesses. Significant deficiencies and material weaknesses must be reported to the company's external auditor and audit committee of the board. Material weaknesses must also be disclosed publicly in the SEC periodic reports. This is one of the most important requirements of the Sarbanes-Oxley Act of 2002 because it puts the responsibility for effective internal controls over financial reporting squarely where it really belongs: company management. In spite of this being such an important compliance requirement to conform with Sections 302 and 404, the Commission has not provided practical guidance to Registrants on how they should do this step.

In the absence of direct guidance from the Commission, the first crop of Section 404 Registrants followed the "back-door" approach – they used the rules external auditors are required to follow to help determine what they should do. The Commission's stance on this issue of relegating the task of developing guidance for Registrants to the PCAOB has been interpreted by many issuers as a grant of absolute authority to external auditors. This power imbalance has led many Registrants to believe they must comply with their external auditors' subjective views on what constitutes effective control and their demands for improvements at any cost. Since management can not disagree with their external auditor's interpretation of the Auditing Standard No. 2 without a high risk of receiving an adverse opinion on their first Section 404 report, they have no choice except to yield to external auditor's demands even to the point where, in the opinion of the

management, the benefits clearly outweigh the costs of such controls. In essence, Commission's lack of direct guidance in this area has created a situation where external auditors now possess wide discretion in subjectively assessing whether a client has, or doesn't have, an "effective" system of internal control.

In our opinion, this guidance imbalance tilts the scale, unjustifiably so, in favour of the external auditors' subjective views on how much control is enough. Considering that PCAOB inspectors are now charged with "second-guessing" the external auditors' work and conclusions external auditors have reached on how much control is enough, it is only natural for external auditors to minimize their reporting risk to the maximum extent possible and pass all additional costs incurred to Registrants. This higher "bargaining power" afforded to the external auditors by virtue of the "back-door" management requirements is one of the major causes of dissatisfaction among SEC Registrants and the high costs being incurred by them to comply with the Section 302 and 404 requirements. One of our clients vented his frustration by observing that "my auditors are printing money on my paper while I am standing there watching them do it." The NASDAQ survey, mentioned in 2.2, cites many comments to support this client's frustrations. It is important to note that we do not fault the approach being taken by the external audit community. They are acting rationally given the situation, particularly in light of the high level of corporate and personal risk attached to incorrectly certifying that internal accounting controls are "effective" – a risk that will, with certainty, materialize in a major way in the near future.

As we see it, the reason the Commission has defaulted to the PCAOB for guidance on how a company should assess and report on the effectiveness of its internal control system over financial reporting is due to the lack of a generally accepted control assessment criteria that managements can rely upon to guide them as they assess, grade, and report on their system of internal control. Had such a set of generally accepted control assessment criteria existed prior to the Sarbanes-Oxley Act of 2002, it would have made perfect sense for the PCAOB to restrict their work to setting auditing standards for external auditors to guide them when evaluating management's process of assessing their system of internal controls and opining on the validity of management's representations (just as external auditors currently opine on the financial statements).

2.4 Too Much Focus on Controls, Not Enough on Risks

Emphasis on examining controls without clear linkage to risks is another factor that is not only driving up costs of compliance but is also leading to very vocal complaints of "shareholder value erosion" and "non-value added" costs by Registrants. The rules as currently written by the Commission and the PCAOB encourage (or arguably require) companies use a "process-centric" or "control-centric" assessment approach to form their conclusions. This is an approach that focuses heavily on detailed documentation of activities and process flows and testing of hundreds of controls. None of the current requirements clearly direct Registrants to start their assessments by first documenting and assessing the key disclosure risks, including assessing the likelihood and potential consequences, that threaten the reliability of the key assertions implicit in all financial statements and note disclosures. Logically one can argue that **only** once the significant risks have been identified and assessed should efforts be made to identify the key controls that are in place to mitigate them. Under the current system, we believe that it is entirely possible for companies to get a clean Section 404(b) opinion from their external auditors without formally documenting and assessing the key risks that threaten the reliability of specific accounts and note disclosures.

This emphasis on controls to the exclusion of risks has resulted in unnecessarily high costs to the Registrants where the focus has frequently been to painstakingly documenting all processes that

feed the accounting and note disclosures and test controls that are often not genuine "key" controls. Key controls are the controls that are actually capable of mitigating real risks that an organization faces in its unique financial reporting environment and the ones that history tells us are really the dominant causes of major financial debacles. More than 70% of the respondents, according to the above-mentioned FEI survey, support risk-based audit approach as opposed to current "control-centric" approach. What the term "risk based audit approach" means to each of these respondents however, is almost certainly highly variable.

Having said that, we must acknowledge that PCAOB Auditing Standard No. 2 (see paragraphs 68-70) does suggest that external auditors shift their focus from "control-centric" audits to "management assertion-centric" audits. Whether the external auditors must focus attention on and ensure the real risks to specific accounts and note disclosures are identified in the process is a point of contention and confusion. Our interactions with the external auditors as well as anecdotal evidence from Registrants tells us that there is a widespread and excessive focus on documentation and "reperformance" of numerous control activities irrespective of whether they effectively mitigate the real risks to reliable disclosures. This clearly indicates that a "risk-centric" approach is, perhaps, not currently being afforded the attention it deserves.

If a decision is arrived at by the Commission to correct this undue emphasis on controls, attention should be paid to develop rules and regulations that would clearly require companies to identify and assess the real and potential risks that threaten reliable accounting disclosures, document the controls that mitigate those risks, and put appropriate systems in place to identify and monitor key performance indicators that provide evidence whether, in fact, the controls in use/place are working and producing a real and potential error rate acceptable to management and the Audit Committee. This type of approach focuses on the acceptability of the current "residual risk status" to management and the Board, not a subjective view of what constitutes an "effective" control system to the external auditor. In light of the external auditor's other primary task of opining on the financial statements, less risk will always be preferred to more risk if all costs can be passed to clients and a profit margin earned. This type of approach would not only reduce costs and non-productive arguments between management and external auditors, but will also provide much needed "legitimacy" to the periodic control assessment process in the eyes of the management. Additionally, the focus on identifying the current residual risk status will force managements to think of financial disclosures as the product of the current control design and that understanding and controlling the error-rate in those accounting disclosure "products" is as important as producing high quality products and services for their customers. In this area, the Basel operational risk reforms in the banking sector and/or the Australian/New Zeeland Risk Management Standard No. 4360 provide a more intellectually defensible approach to governance that focuses on what is really critical – the acceptability of the residual risk situation produced by the controls or "mitigators" that are currently in use -- to management, the audit committee and the external auditor.

2.5 Meaning of "More than Inconsequential" and "More than Remote"

Most professionals that are involved in this area agree that, when compared with the "reportable condition" mind-set (as per SAS #60), Auditing Standard No. 2 has lowered the thresholds for grading and reporting control deficiencies. Management as well as external auditors are struggling to get a handle on what exactly constitutes "more than inconsequential" and "more than remote." Repeatability in reaching the same conclusion given the same set of circumstances is often missing. (Note: Our field tests validate this conclusion.) Even though, the SEC and PCAOB have referred the Registrants and the auditors to FAS #5, SAB #99 and other related references (i.e. Version 3 of the Guidance Released by the 9 CPA Firms) to seek guidance on

how to "operationalize" these two contentious criteria. The reality is that more than a few external auditors are documenting and reporting relatively low level procedural deficiencies as serious control deficiencies This is true in spite of the fact that external auditors continue to give clean opinions on the reliability of the numbers being reported in hundreds of Registrants where management and/or the auditor reported "material" weaknesses. Our conversations with the external auditors reveal that they agree that such procedural deficiencies did not cause Enron and will not stop WorldCom like debacles going forward. Unfortunately, under the current guidance, they have no choice except to document and report these relatively low level control deficiencies because it is very difficult to make an argument against the view that a discovered internal control weakness could be "potentially" more than inconsequential or less than remote. Additionally, just as determining materiality in a financial-statement audit context has historically proven to be a difficult and elusive concept, the "more than inconsequential", or the exposure dimension of grading and reporting internal control weaknesses, is proving to be much more contentious and more difficult than had been anticipated. Consequently, given the fear of regulatory sanctions and "second-guessing" of auditors' work by the PCAOB inspectors, the potential for class-action lawsuits, and the absence of clear guidance, it is not surprising that external auditors, to protect themselves from any potential challenges in the future, have set materiality thresholds to levels of materiality where we believe the costs of debating whether these issues constitute "material weaknesses" often outweigh the benefits of the information reported. Further, as mentioned earlier, emphasizing controls and not addressing the notion of "residual risk", the risk that still remains that could result in a material error, while conducting control assessments exacerbates this problem all the more.

Although, the Commission is seeking feedback only on the Section 404 implementation experiences, we would like to take this opportunity to bring to Commission's attention other important issues related to Sections 302 and 404 that we believe are also contributing to the current confusion.

2.6 Inconsistencies in Section 302/404 wording vis-à-vis Commission's Final Rules

Following are some inconsistencies that we see between what we believe Congress intended in Sections 302 and 404 of the Act and what the respective SEC Final Rules suggest.

- Section 302 applies to both quarterly and annual reports filed by Registrants with the SEC. The strict and literal interpretation of the sub-sections (a) (4) and (a) (5) of the Section 302 calls for a full reassessment of control effectiveness by management four times a year and reporting of all significant deficiencies and material weaknesses that are discovered each quarter to the audit committee and external auditor. However, in the Final Rule issued for Section 404, the Commission indicated that it would not require the full quarterly control effectiveness assessments called for in Section 302. Following is the specific language used by the Commission to alter the intent of Section 302:

  > After consideration of the comments received, we have decided not to require quarterly evaluations of internal control over financial reporting that are as extensive as the annual evaluation……. Accordingly, we are adopting amendments that require a company's management, with the participation of the principal executive and financial officers, to evaluate any change in the company's internal control that occurred during a fiscal quarter that has materially affected, or is reasonably likely to materially affect, the company's internal control over financial reporting. (See Section C.3 of the Final Rules on Section 404).

It isn't clear from the above-mentioned wording if the Commission, by waving the requirement for full quarterly assessment of internal controls over financial reporting, also suspended the need to report significant deficiencies and material weaknesses each quarter to the audit committee and external auditor as well as the requirement to disclose new material weaknesses that come to light in quarterly control effectiveness certifications to the SEC. One could conclude that a newly detected material weakness during a quarter is a material change in control, but would one consider it a material change in control even when that condition existed earlier but the Registrant only detected it's severity and impact during the current quarter.

Many Registrants do not know what the apparent contradictions between the literal wording of the Act and the SEC Final Rules mean in practice, or where exactly the law really stands today. The wording in Section 302(a) (4) (D) implies that disclosure of control deficiencies identified by management during their quarterly assessments should commence with the effective date of Section 302. Even though the SEC Final Rule for Section 302 was effective from August 29, 2002, many Registrants concluded that they did not need to report known control problems until their first section 404 reporting date, in spite of continuing to confirm in the SEC filings that the company has an "effective" system of disclosure control. We are unaware of the support for this conclusion.

- The Commission has confirmed that the requirement that management must assess the effectiveness of "disclosure controls" each quarter and report related conclusions is in full force. "Disclosure controls", according to the Commission, are to be distinguished from the internal controls that ensure reliable financial reporting. (Note: Financial statements are a key disclosure made each quarter by all the Registrants.) The distinction between disclosure controls and internal control over financial reporting is subtle and difficult to make in practice. From a practical perspective, the problem is that, if each quarter material changes in internal controls over financial reporting must be disclosed and new significant deficiencies and material weaknesses must still be reported per Section 302 to the audit committee and the company's external auditor, it would only seem logical that the quarterly analysis of disclosure controls must also ensure that there are effective internal control systems over financial reporting in place to accomplish these two requirements. The key question that remains is, given the SEC requirement to assess "disclosure controls" each quarter is still in full force, does it also include proactively assessing the internal control systems in place to identify material changes in internal controls each quarter and situations where the conclusion on control effectiveness for Section 404 has proven to be inaccurate or incomplete by the passage of time? For example, surfacing of major problems in the second-quarter with the accuracy of financial numbers reported at year-end would call previously reached Section 404 effectiveness conclusions into question. In other words, should such circumstances invoke a full reassessment of internal control effectiveness at a Registrant?

- At a technical level, the wording in Section 302 (a) (5) (A), strictly interpreted, requires that significant deficiencies in internal controls over financial reporting must be reported to both the audit committee and the company's external auditor. However, although it is clear from the wording in the section that the external auditor should be told about any material weaknesses in control, it isn't clear from the wording that the audit committee should also be told about them – an obvious anomaly in the drafting that appears to run counter to the intent of the Sarbanes-Oxley Act. Although, the Final Rule for Section 302 is silent on this issue, the Final Rule for Section 404 clarifies or, perhaps more bluntly, corrects the intent of the Congress in the Act by requiring that both significant deficiencies and material weaknesses should be reported to the company's external auditor and audit committee. However, what is

not clear, at least to us, is whether this is to happen quarterly or only annually because this clarification comes from the Final Rules for Section 404 and the Section 404 applies only to the annual reports required by section 13 (a) or 15 (d) of the Securities and Exchange act of 1934.

- The other problematic element of Section 302, beyond the confusion on the frequency with which management must proactively identify and report significant deficiencies and material weaknesses, is the new obligation imposed by the Commission as a substitute for full quarterly re-assessment in Section 404 Final Rule to identify "…any change in the company's internal control that occurred during a fiscal quarter that has materially, affected, or is reasonably likely to materially affect, the company's internal control over financial reporting" (see Section C.3 of the Section 404 Final Rule). Identifying changes that "materially affect" internal controls over financial reporting is not the same as identifying new reportable control deficiencies. It can also mean disclosing areas of the internal control system that were considered adequate before but are now much stronger. Nothing in the Final Rules indicate that only deficiencies should be disclosed. It can also mean identifying information on the current reliability of accounting processes that calls in to question conclusions reached at the prior year-end on internal control effectiveness. This is a new SEC imposed reporting requirement that will create confusion and controversy as Registrants prepare to deal with the first quarter assessments after their initial Section 404 reporting. There is currently no guidance on how this step should be accomplished that we are aware of, especially on the key issue of what constitutes a "material change". Our clients are already starting to ask us with increasing frequency what guidance is available to them that defines what is meant by the term "material change" as they prepare to report on their first quarterly assessments subsequent to their first Section 404 report. Our answer has been that there is no guidance currently available from the SEC to the best of our knowledge. Since external auditors are not required to report on the support for these certifications, the Commission cannot reasonably expect the PCAOB to compensate for the absence of clear guidance in this area.

3. Recommendations to Consider

Listed below are some proposals that, in our opinion, could help avoid many of the dysfunctional consequences that have occurred as a result of the way the Sarbanes-Oxley Act of 2002 has been interpreted and implemented to date without losing its many positive aspects and impacts.

3.1 Require that Registrants and Auditors Focus on the Acceptability of Residual Risk

Currently a great many companies that are using the guidance in Auditing Standard #2, and/or acting on the advice of their outside advisors, are using a "process-centric" or "control-centric" approach to their Section 302 and 404 compliance efforts, often with only limited or even no linkage to the real risks that have caused or have the potential to cause accounting misstatements. Using a risk based approach, specific accounting line item and note disclosures are stated as objectives (e.g. ensure inventory disclosure is reliable, ensure accounts receivable disclosure is reliable, ensure the legal proceedings note disclosure is reliable, and so on). Users then proceed to document the significant risks that threaten the reliability of those accounts or note disclosures. What the profession has historically called "management assertions" such as existence or occurrence, completeness, rights and obligations, valuation or allocation, and presentation and disclosure form the primary basis for these risks (e.g. a risk to the reliability of inventory disclosure is that it doesn't even exist). These "assertion risks" must often be customized and supplemented with risks specific to the industry and company. Only after the key assertion risks have been identified and ranked should efforts be made to identify and document the key controls

in place to mitigate such risks. Under this approach it is not necessary to document all activities in all related supporting processes. The concept of "key controls" still remains valid but under this approach it is contextualized and grounded in identifying controls that help mitigate the key or significant risks. "Key controls" are the controls that mitigate the most significant risks or mitigate risks **most efficiently and effectively**. The next step is to document information that helps management and external auditors understand the current residual risk situation. This should include documenting real or potential situations where the controls in use/place are not likely to be effective. The real goal should not be to spend massive amounts of time debating whether controls are, or are not effective. It should be on debating whether the current residual risk situation is acceptable to the management and the audit committee. **As long as the external auditor is fully aware of the current residual risk status they should be equipped to determine what additional audit steps they should take to compensate for the current deficiencies in client's system of internal controls.** This approach has the potential to significantly reduce audit risk – the risk of external auditors giving an incorrect opinion on financial disclosures. We think it is this goal that should be the focus of sections 302 and 404

3.2 Retain the Requirement to Develop and Maintain Control Design Documentation

The requirement that companies develop and maintain reliable risk and control analysis and documentation related to internal accounting control disclosures should be maintained. The fact that so many companies had not developed risk and control assessment documentation related to their internal accounting control disclosures prior to Sarbanes-Oxley Act of 2002 indicates that potentially thousands of senior executives were, and are in other countries today, signing accounting control declarations with limited or, in some extreme cases, no formal risk and control assessment and testing documentation to support their claims. Although the cost of creating risk and control assessment documentation can be significant, particularly in the first year, this element should continue to be mandatory. We believe that going forward the cost to up-date this documentation should be relatively modest. Further, the use of appropriate technology platforms to store and maintain risk and control assessment documentation would make this process even less onerous and more integrated with other internal reporting needs of the Registrant.

3.3 Require Companies Update Control Design Documentation Quarterly

Section 302 of the Act explicitly calls for quarterly representations on control effectiveness and quarterly reporting of significant deficiencies as well as material weaknesses by company managements to external auditors and audit committees. This requirement was modified by the Commission and replaced with a requirement that for quarterly reporting management need not do a full reassessment and, instead, identify and report only "material changes" in the company's controls. The requirement that management certify in SEC filings that significant deficiencies and material weaknesses have been reported to the company's external auditor and audit committee each quarter has been retained, albeit in a somewhat confused state currently. Based on our experience, we believe that the requirement to identify material changes in control, while it was proposed by the SEC as a way to reduce Sarbanes-Oxley compliance costs, will actually create significant additional confusion and unnecessary costs. We are seeing a rapid escalation in the confusion related to this issue as companies turn their attention to it following their first section 404 report. We recommend that management be required to certify that they have a process in place (following their first full Section 404 report on control effectiveness) to update their control assessment design documentation each quarter, a process to identify new control incidents or events that provide information on actual control effectiveness, and a process to identify and report any new significant deficiencies and/or material weaknesses detected as a result of that update activity and new information that has surfaced on control effectiveness. Quarterly testing

to confirm the operation of controls identified in the control design documentation should not be mandatory; however a company may wish to do testing throughout the year to support their Section 404 control effectiveness certification. Once a company's first set of control assessment documentation is in place this requirement should not be overly costly.

3.4 External Auditors Should Audit the Process Used to Identify and Report the Current Residual Risk Status to Senior Management, the Audit Committee, and to Themselves Including the Reliability of Control Status Reports. Major deficiencies in either the process or status reports should be reported as a "Material Weakness in Management's Assessment Process"

The external auditor should evaluate the risk and control assessment process used by management, (i.e. the reliability of the framework in place to identify and report the current residual risk situation) and be required by the PCAOB to test the reliability and completeness of the residual risk status information (i.e. substantively verify that the results reported on the current risks being accepted in light of the controls in place are reliable) Any situation detected by the external auditor where the auditor concludes that it is a conscious misstatement of either the control design documentation or control testing results should be immediately classified as a significant deficiency and reported to senior management and the audit committee pursuant to the fraud reporting requirement in Section 302(a)(5)(B). A pattern of conscious misstatements of either control designs or control test results should be classified as a material weakness in the Registrant's control environment that management must report to the SEC. Deficiencies in management's control design assessment work and control operations testing that are **not** deemed by the external auditor to be conscious acts (i.e. those linked to skill deficiency and/or coverage) should be graded and reported to management and the Audit Committee based on their severity and frequency. Major deficiencies should be reported to the SEC.

We believe that this approach will result in a very significant reduction in the ongoing cost of complying with Sections 302 and 404. Additionally, this approach will reinforce the importance of maintaining reliable control assessment documentation and focus attention on the competence and integrity of management – two key elements to reliable financial disclosures. Under this scenario, when the external auditor determines that any element of management's internal control assessment is unreliable they should be allowed to do the amount of additional work they consider necessary to independently form an opinion on Registrant's current internal control effectiveness over financial reporting and to support their opinion on the company's financial results. The cost of additional work done by the external auditors due to the discovery of material deficiencies in the internal control assessment conducted by the management should be disclosed to the audit committee. External auditors should be provided with explicit guidance by the PCAOB to deal with situations where the control deficiencies and/or control assessment process deficiencies are so severe that they cannot or should not provide an opinion on the financial accounts and notes. Moody's, the credit rating agency, refers to these situations as Category B control deficiencies. These safeguards will deter the auditors from constantly "auditing around" major deficiencies. More than a few people, and all three of the major credit rating agencies, are now questioning how external auditors can form a positive opinion on the reliability of the accounts and note disclosures when there is documented evidence of severe and pervasive problems in a client's control environment.

3.5 Going Forward Need to Provide Flexibility to Management to Determine the Level of Control Testing Necessary to Support its Assessment Conclusion

As is currently the case, almost all Big-4 public accounting firms and many of the smaller firms have established minimum control testing frequency requirements. For various reasons (e.g., fear of litigation, "second-guessing" of the audit process by the PCAOB inspectors etc.) these minimum sample sizes are often made "mandatory" for all internal test samples done by management by their external audit firm irrespective of Registrant's state of internal control assessment effectiveness. Rather than external auditors mandating specific control testing frequencies that management must conform to, regardless of the effectiveness of their internal control assessment structure, management should be allowed to determine how much testing of internal controls they believe needs to be done to produce and maintain a complete and reliable internal control effectiveness assessment process. For example, in companies where (1) Registrant staff is highly skilled in developing and maintaining reliable control assessment documentation, and (2) those responsible for operating and overseeing the controls are truthful and candid in disclosing any changes in risks, control design and all relevant and necessary information on the actual operation and effectiveness of internal controls (i.e. the residual risk status), the amount of testing necessary to verify management representations should be significantly lower than that required for companies where the staff responsible for Sarbanes control assessment documentation are poorly trained, lack integrity or can not be relied upon based on various other reasons. If management makes poor decisions on the amount of control testing necessary to produce reliable control effectiveness assessments for Sections 302 and 404 it will reflect in the audit opinion on their assessment process and the conclusions arrived at by their external auditor on the reliability of the assessment and conclusions (i.e. they will be proven wrong or challenged by the external auditor on the quality of the support for their conclusions). Staff responsible for the operation of the controls identified in the control design documentation should be responsible for confirming that the controls operated as described and disclosing any controls operations exceptions. Any employee or third party acting for the company that consciously misstates control assessment documentation, including the frequency and execution of a documented control, should be reported to the audit committee. A pattern of such behaviour should result in management having to report a material weakness in their control environment controls in their various SEC filings.

This approach should allow the management to adjust the amount of testing it undertakes to confirm the reliability of their control assessment documentation and control status representations. We believe that this recommendation has the potential to significantly reduce the overall Sections 302 and 404 compliance costs in companies that make a good effort to produce reliable control effectiveness assessments and maintain a strong control environment. Companies that lack commitment to providing their audit committee, the external auditors, and the Commission with reliable control effectiveness assessments will be identified and penalized through additional external audit costs and public visibility on the quality and integrity of their control assessment disclosures.

3.6 Provide Guidance for Management on How to Assess and Report on Control Effectiveness

Currently the primary source of guidance for management to prepare and confirm control assessment documentation is PCAOB Auditing Standard No. 2. As described earlier, this is not optimal. The focus of Auditing Standard No. 2 should be on describing the audit standards to be applied by the external auditor to form an opinion on the reliability of management's control effectiveness assessment and financial disclosures. Audit standards written for external auditors

do not constitute appropriate and sufficient guidance for use by management. They should only provide auditors with a basis for auditing the reliability and completeness of management's process and representations just as they audit the reliability and completeness of the income statements and balance sheets produced by management. A completely separate source of guidance similar to that described in Basel II for managing operational risks in banks, the guidance for Malcolm Baldrige, or the guidance produced by the FASB in the case of GAAP is required to guide management in developing a framework for establishing and sustaining appropriate internal controls over financial disclosures. Clearly written guidance on acceptable methods to identify, grade and report on residual risk status, including existing control deficiencies (i.e. real or potential situations that plausible risks will not be mitigated) will help reduce compliance costs, minimize the amount of non-productive debates and disagreements between management and external auditors, and firmly establish management's accountability to consistently produce reliable control assessments and financial disclosures.

As we discussed earlier in this comment letter, the biggest hurdle that the COSO control model must overcome to make it an acceptable control assessment model, is repeatability of assessment conclusions reached using its framework. The new COSO ERM framework shows promise but has seen limited genuine acceptance to date. We believe that the COSO organization as it currently exists is understaffed and lacks the resources and mandate to do what is necessary in this critical area. Either COSO's ongoing mandate as the primary agency responsible for producing guidance on control assessment criteria and methods should be legitimized or a new not-for-profit organization similar in structure to the PCAOB be commissioned to develop and continuously improve financial accounting control assessment standards and guidance. Further, considering that rest of the world is following in U.S. footsteps by starting to enact "SOX-like" legislation, the Commission should consider taking a global perspective and take a leadership position to establish an international consortium that would include company representatives, academics and audit practitioners from various interested nations to develop internationally recognized and generally accepted accounting control assessment criteria and guidance. Given that national accounting standards have proven to be costly and create confusion globally, logic would suggest that the same mistake should not be made in the area of accounting control assessment standards.

3.7 SEC Should Release Clear Guidance on How Registrants should Report on Control Deficiencies and Related Remediation Actions

Our review and detailed analysis of more than 500 SEC control deficiency filings indicate to us that, at least in the pre-Section 404 reporting period, the quality and quantity of information being reported on control deficiencies has been generally poor. Although one of the goals of the Sarbanes-Oxley Act of 2002 is to improve corporate financial reporting by enhancing transparency in the disclosures, the control deficiency disclosures filed with the Commission in 2004 were often poor quality. For example, the filings often lack a clear description of what risks are currently not being mitigated adequately, which account or note disclosures in SEC filings are impacted or are at risk of being wrong, and/or which COSO control category is involved. From the perspective of an investor, the control deficiency disclosures often do not say what happened or what went wrong in a clear and understandable way. Similarly, the corrective actions identified often do not clearly describe how the Registrant has fixed the problem and why the control deficiency will not be repeated in the future. It will be a shame if, after all this effort and cost, investors are left wondering about the state of effectiveness of internal controls a Registrant has over its financial reporting and the reliability of the external auditor's conclusions on the numbers. The fact that external auditors appear, at least so far, to be signalling that they believe they can form defensible opinions on the reliability of the accounting disclosures regardless of the

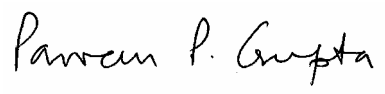
severity of the control problems compounds this situation. It is important that the Commission evaluate and monitor Registrants' quality of disclosure in this area and the PCAOB inspectors keep the public accounting firms "on notice" to ensure external auditors demand open and forthright disclosure of material weaknesses, along with sufficient description of the remediation actions from their clients to achieve the ultimate objective of the Act: enhancing trust, faith and confidence in our financial markets.

We sincerely hope the Commission will consider our observations and recommendations as it deliberates on reforms aimed at balancing the costs companies are currently incurring to comply with the Act with its intended benefits. We will be more than happy to discuss our observations and recommendations in more detail, in person, including presenting real life cases to illustrate the basis for our conclusions and recommendations at your convenience.

Respectfully Submitted

Tim Leech
Chief Methodology Officer
Paisley Consulting
2655 North Sheridan Way, Suite 150
Mississauga, Ontario, Canada L5K 2PB
Tim.Leech@paisleyconsulting.com

Respectfully Submitted



Parveen P. Gupta
Magee Distinguished Professor of Accounting
Lehigh University
621 Taylor Street, RBC #37
Bethlehem, PA 18015
ppg0@lehigh.edu

cc: Mr. William H. Donaldson, SEC Chairman
Mr. Paul S. Atkins, SEC Commissioner
Mr. Roel C. Campos, SEC Commissioner
Ms. Cynthia A. Glassman, SEC Commissioner
Mr. Harvey J. Goldschmid, SEC Commissioner
Mr. Donald T. Nicolaisen, SEC Chief Accountant
Mr. William J. McDonough, PCAOB Chairman
Dr. Douglas R. Carmichael, PCAOB Chief Auditor
Ms. Laura J. Phillips, PCAOB Associate Chief Auditor
Mr. Thomas Ray, PCAOB Deputy Chief Auditor