INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

February 13, 2007

Re: SEC File No. S7-24-06 and PCAOB Rulemaking Docket No. 021

The **Institute of Management Accountants** applauds the efforts made to date by the SEC and PCAOB to make SOX implementation more cost-effective and practical while still protecting investors. We are pleased to continue sharing our extensive global research and recommendations with the SEC, PCAOB, professional accounting associations, the trade media, the U.S. Chamber of Commerce, Members of Congress and other security regulators around the world interested in this issue.

IMA's conclusion, after careful consideration of the SEC and PCAOB December 2006 proposals, is that significant additional actions are required to optimize the cost/benefit equation. This letter contains a **main body (7 pages)** and **3 attachments** (Attachment 1 – IMA Risk-Based Framework; Attachment 2 – Technical Analysis of SEC Guidance; Attachment 3 – Technical Analysis of PCAOB draft audit standard).

We have summarized below the five interrelated issues that we believe remain to be addressed, together with our technical analysis and recommendations for change. These five issues have been identified through extensive research and careful consideration of the reasons cited by Canada, the EU and Japan for not fully adopting the current U.S. SOX regulations.

- **Issue 1**: Two rule books (SEC, PCAOB) for the same assessment task – a recipe for unintended confusion and complexity. In short, without major changes to the draft rules ASX/5 will likely replace AS2 as management's de facto standard.
- **Issue 2**: The proposals are not risk-based by global risk management standards, reducing the benefits that could accrue from an assessment approach that focuses on identifying specific significant risks and understanding residual risk status.
- **Issue 3**: The current "quality bar" of zero material defects in draft financial statements is expensive without significantly increasing investor protection. This situation is compounded by the current requirement that identification of even one material control weakness requires management publicly report ineffective ICFR.
- **Issue 4**: The draft proposals call for elimination of the audit opinion on management's ICFR assessment process and retention of the auditor's subjective opinion on ICFR effectiveness. While some agree with this interpretation of the Act, it is contrary to IMA's and IIA's publicly reported views, some early comment letter responses, and the current stance of the U.S. federal government, Japan, Canada, and the EU capital market regulatory bodies.
- **Issue 5**: The draft proposals are still not practical for smaller public companies – all four issues listed above disproportionately impact smaller public companies.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

<table>
<tr><th>Issue #1/Impact</th><th>What Needs to Change</th></tr>
<tr><td>
Two rule books for the same task – a recipe for unintended confusion and complexity.
The SEC proposed rule is high level and broad to the point of being vague on minimum expectations in a number of key areas, including but not limited to the need to specifically identify, document and assess major risks and residual risk status. The PCAOB standard is more granular, prescriptive and control focused. The PCAOB rules constitute the "exam grading rule book" auditors must use or risk severe PCAOB sanctions and increased litigation exposure.
Because under the current proposals auditors will still determine ICFR pass/fail rating, PCAOB rules will likely continue to be the de facto rule book for management that want a passing grade. This is a sub-optimal situation and contrary to what we believe is the true intent of the Act.
A few examples of the more significant differences and/or inconsistencies that exist between the SEC and PCAOB proposals include:

Control Environment Evaluation – ASX/5 indicates that the auditor should assess the company's control environment and lists 5 specific areas for attention. The SEC guide makes passing reference to the concept but does not provide specific evaluation criteria or any information on what would constitute a failing grade on control environment.
Identifying Significant Accounts – ASX/5 lists 9 specific factors that should be used to identify significant accounts. SEC guidance has no parallel guidance for management.
Strong Indicators of Material Weakness – ASX/5 lists almost 3 pages of specific factors that are relevant to determining if a material weakness is present. The SEC guidance starting on page 41 provides similar but different criteria to be used by management.

</td><td>
The SEC guidance should be the only ICFR "how to" assessment guidance.
Management teams that follow SEC interpretative guidance should be fully entitled to say they have done what is expected of them without fear of being overruled and/or contradicted by the more prescriptive, granular and control-centric PCAOB rules. Although the SEC proposed rule states that this result is indeed a goal, we believe that management will have to use and conform to the PCAOB rules in order to satisfy their external auditors.
When revisions to the draft PCAOB standard are done following the comment period, we recommend all sections that describe how to complete an assessment of ICFR should be deleted from the Standard and auditors directed to use the same SEC interpretative guidance used by management.
The focus in ASX/5 should be solely on audit considerations. However, the SEC primary ICFR assessment guidance should be revised to reflect IMA recommendations made in Issues 2-5 below.
</td></tr>
</table>

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Issue #2/Impact	*What Needs to Change*
The SEC proposed rule and PCAOB revised standard are still not top-down/risk-based by global risk management standards. If these documents were truly top-down/risk-based users would be encouraged and allowed by the SEC to use globally accepted risk assessment frameworks such as AS/NZ 4360, COSO ERM, or the IMA top-down/risk-based ICFR assessment framework proposed in September. Application of any of these approaches would require that assessments start by formally documenting and assessing significant risks at both the entity and account/note level - risks that are already known to have resulted in materially unreliable financial statements. We would argue that this level of guidance is the appropriate balance between ambiguity at one extreme and prescription at the other. Although there is some reference to this step in the SEC guidance this step is not emphasized sufficiently or clearly enough. No examples or guidance on how to complete this step are currently in either set of draft rules. It is also important to note that nowhere in the SEC or PCAOB draft guidance do the authors use the words "residual risk" or "residual risk status". Identification and assessment of residual risk is a key element of any true risk-based assessment methodology and a cornerstone of all internationally recognized risk management standards. For example, the PCAOB proposed standard on page 5 directs auditors to start by examining and testing company level controls without first carefully identifying and assessing entity-level risks. In contrast, the SEC guidance alludes to starting with risks but does not take advantage of globally accepted methods to provide some level of practical "how to" guidance.	**Both the SEC and PCAOB proposals should be rewritten to reflect and require a true top-down/risk-based ICFR assessment approach. We are seeking "balance, not bias" between risk and controls-based methods.** A true top-down/risk-based approach starts with management identifying major risks at the entity level that are already known to be primary causes of material financial statement errors. Controls in place to mitigate these statistically predictable risks are then documented and specifically linked to the risks identified. Management must decide whether to mitigate the significant risks identified using controls, share or transfer risks using vehicles like outsourcing and/or insurance, accept the risk, or avoid the risk entirely. Residual risk status, including current detected error rates, is identified, documented and assessed by both management and auditors. Auditors are entitled and expected to adjust their audit approach to fully compensate for any retained ICFR residual risks the company has decided to accept. In severe cases where the ICFR systems in place exhibit levels of residual risk totally unacceptable to the company's auditor, they have the right and ability to refuse to provide an opinion on the company's financial statements and/or resign from the engagement. Well-run and tightly controlled companies will be rewarded with a lower cost of capital and significantly lower audit fees relative to companies that prepare poor quality ICFR assessments and/or accept higher levels of ICFR residual risk. **IMA's top-down/risk-based ICFR framework is included as Attachment 1 to this letter with greater detail available at**: www.sec.gov/comments/s7-11-06/s71106.shtml

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

<table>
<tr><th>Issue #3/Impact</th><th>What Needs to Change</th></tr>
<tr><td>

The draft financial statement and ICFR "quality bars" are set too high, resulting in high cost without a commensurate increase in investor protection.

Current SEC and PCAOB regulations require management produce draft financial statements with zero material defects for their external auditors or risk being publicly labeled in SEC filings as having "ineffective" ICFR. This is a complex issue that is directly linked to Issue 4 below. We believe that retaining the audit opinion on control "effectiveness" combined with the high quality bar on draft financial statements and ICFR is a dangerous mix.

It is important to note that zero material defects is a level of draft financial statement quality and ICFR that is not currently expected, or required, by capital market regulators anywhere else in the world, including Canada, the UK, Europe or Japan. While zero material defects in ICFR and financial statement drafts prepared by management is a laudable "goal", we believe that it is a level of perfection that will result in the U.S. being at a competitive global disadvantage relative to countries viewed as having similarly reliable corporate governance systems without this requirement.

In January, 2007 the McKinsey Report "Sustaining New York's and the US' Global Financial Services Leadership" study referenced the UK regulatory approach of discussing (draft) issues constructively and not penalizing companies for proactively coming forward with a potential issue; by contrast, in the U.S. "executives by and large are hesitant to raise even minor problems with regulators for fear that simply broaching the subject will lead to immediate enforcement action or, worse yet, a highly charged public prosecution".

</td><td>

Allow companies to have ICFR systems that are less expensive than zero material defect systems. Require, via specific PCAOB auditing standards, that auditors adjust their work to fully compensate for control deficiencies identified by management and, in cases where management's ICFR assessment work was not rated as fully reliable, their own supplemental ICFR analysis. Auditors should publicly report on the reliability of management's ICFR assessment process (see Issue 4).

We believe that the primary goal of management's assessment of ICFR should be to clearly identify and candidly report areas of significant residual risk (using robust quality management systems) to the company's audit committee and external auditors. Using this type of approach external auditors audit and report on the reliability of the risk and control assessment <u>process</u> maintained by management.

Auditors are required to modify the scope and extent of their substantive audit work to compensate for any areas of residual risk currently being accepted by the company's management and audit committee. Any errors identified in the draft financial statements by the company's auditors must be corrected by management prior to filing the accounts with the SEC. The frequency and magnitude of auditor detected errors in drafts prepared by management should be an important input to auditor opinions on the reliability of management's ICFR assessment process.

A Glass & Lewis research study published in June 2005 provided clear evidence that literally hundreds of U.S. public companies claimed to have fully effective disclosure and ICFR systems right up to the point in time auditors had to provide an opinion on the reliability of their assessment work. At that point in time management, under the zero material defect rule, had to acknowledge material ICFR deficiencies existed. Good regulation should result in providing <u>positive</u> incentives to management to be candid and proactive in identifying issues in the financial statement drafting process.

</td></tr>
</table>

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Issue #4/Impact	*What Needs to Change*
Misapplication of what we believe was Congress' intent in Section 404 (b), resulting in external auditors duplicating management's accountability for controls testing and assessment. Section 404 (b) of the Act states: "With respect to the internal control assessment required by sub-section (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer …". We do not believe that it was the intent of Congress to require that a company's auditor provide their own subjective view on whether control is or is not "effective". IMA research and other studies demonstrate that current ICFR standards and frameworks are not mature enough to produce repeatable conclusions on controls effectiveness. In other words, we do not believe that any framework is "fit for purpose" in terms of the SEC's four suitability criteria which include repeatability, sufficiently complete, free from bias and relevance. Revenue generation opportunities combined with a litigious environment provide tangible incentives for auditors to "raise the control bar". While this is a contentious issue, we fully support what we believe is the true intent of 404 (b) – an independent report on whether management is taking the responsibility assigned in section 404 (a) seriously and conscientiously. There is growing support for IMA's stance on this issue: 1. Global regulatory regimes that have carefully studied the U.S. SOX regime and chosen not to include the audit opinion on effectiveness (e.g., Japan, Canada and the U.K.), 2. The public position taken on the issue by the Institute of Internal Auditors, and 3. The comment letter from The Alamo Group, a $400M accelerated filer.	**Eliminate the costly and subjective audit opinion on controls effectiveness but retain/strengthen the audit opinion on management's assessment process in the context of a true risk-based approach**. Our basis for this recommendation is that current frameworks are not fit for purpose in making the pass/fail effectiveness conclusion, the process is costly and inefficient, it de-emphasizes management's accountability, and further increases the enormous litigation exposure of auditors (passed on to management in the form of higher fees). Additionally, an audit of management's (true) risk-based assessment process is more likely to uncover fraud (<u>leading</u> indicator of material weakness vs. <u>lagging</u> indicator of controls effectiveness). We recommend instead that the company's auditors audit and report on whether the company's management "has conformed, in all material ways, with SEC requirements to complete a top-down/risk-based ICFR assessment and reported the results to the company's audit committee and to us, the company's external auditors". This process would include careful analysis of residual risk status (the risk remaining after considering risk treatments) by both management and external auditors. It is important to note that the need for a redefined Section 404 (b) is building globally. Preliminary evidence suggests that, unfortunately, in countries where there is a requirement that management publicly report on ICFR – but, without a requirement for the auditor to report on the quality of that work – some companies do very little formal assessment work to support their public representations. The situation is even worse in countries that have no mandatory requirements for management to assess and report on ICFR. Canadian securities regulators have explicitly acknowledged this very real risk and are currently monitoring the situation to determine if corrective steps are necessary. We believe that audit opinions issued should reference the revised SEC guidance for management as the benchmark.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Issue #5/Impact	*What Needs to Change*
The draft regulations are still not practical or scaleable for smaller public companies. ("SPCs") As one example, control structures capable of achieving zero material defects in draft statements are very expensive - money that is often better directed in SPCs to growing the company and producing increased shareholder value. All four issues described above disproportionately impact smaller public companies. It is important to note that the AICPA in the U.S. and audit standard setters in countries like Canada, the UK and Europe continue to believe and assert, correctly or otherwise, that auditors can produce a level of audit opinion quality and reliability on financial statements on par with SOX audit opinions without the use of a SOX-like assessment of ICFR. Investors are not currently being explicitly told that there is any differential in audit opinion quality on audited financial statements (e.g., non-accelerated vs. accelerated, public companies vs. private, etc). There is currently no empirical research we are aware of that validates the premise of differential audit quality. The recent study commissioned by the City of New York prepared by McKinsey & Company has recommended that U.S. listed SPCs be allowed to "opt out" of current PCAOB audit requirements but be required to make conspicuous disclosure of the risks that come with less emphasis on ICFR and potentially lower audit opinion reliability. We respectfully do not agree with the study suggestion that SPCs be allowed to opt out of SOX because of the implications of a "grade B" audit opinion, but we do understand the motivation. It is important to note that the U.S. government has, itself, not adopted a requirement that auditors provide opinions on the effectiveness of ICFR in federal departments and agencies at this point.	**We believe that if all four primary issues above are addressed "disproportionate *benefits*" will accrue to smaller public companies**: one set of assessment rules with management in the lead; a practical and scalable risk assessment process; and, setting the quality bar for material defects in financial statement drafts at a reasonable level combined with auditors opining on the assessment process (and not the pass/fail subjective audit opinion on effectiveness). In addition to generally increasing the practicality of the SOX rules through the reforms we are proposing, the skills and tools necessary to complete true risk-based/top-down assessments can be used in companies of all sizes and types not just for ICFR. They can be applied to other key areas like product quality, customer service, safety, cost control, revenue generation and other areas key to longer term business success. This helps improve the overall ROI of a true risk-based approach for all types of organizations. With due respect to the preeminent committees that have examined this issue, we do not believe that any public company should be exempted from section 404(b) of the Act but do believe the interpretation of the section should be redefined. Investors should be provided with information on the quality of the assessments prepared by management – a very good indicator of ICFR assessment skill and "tone at the top". This should include assessments made on the quality of operations driven by a robust QMS (Quality Management System). The mantra "building quality in" better enables sustainable financial reliability. Additional research on audit opinion reliability with, and without, ICFR assessment and audit assurance on management's ICFR assessment process should be initiated by the SEC, PCAOB, and/or the AICPA as soon as possible. If audit opinions produced under the SOX reporting regime prove to be no more reliable than Canadian or UK audit opinions that do not require similarly costly audit assurance on ICFR, Congress should reevaluate the cost/benefit of section 404(b).

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

IMA solutions-oriented resources available to practitioners include:

1. **IMA Research Study**: "Internal Control: COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices", Professor Parveen Gupta, LLB, Ph.D.

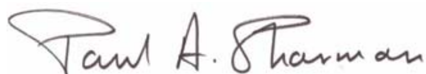
2. **IMA Discussion Paper**: "A Global Perspective On Assessing Internal Control Over Financial Reporting" submitted to the SEC 9/15/06.

3. **IMA Statement on Management Accounting**: "Enterprise Risk Management: Frameworks, Elements and Integration" released January 17, 2007. Professor William Shenkir, Ph.D.,CPA, Professor Paul L. Walker, Ph.D.,CPA. A second SMA focused on ERM Tools and Techniques ("how to") will be available in the early Spring of 2007.

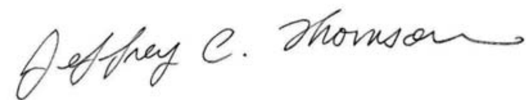
The IMA is a global organization representing a diverse constituency and as such the observations and recommendations in this letter are meant to have broad application in the private and public sectors in countries around the world. This comment letter went through a formal exposure process with the IMA membership.

We would be pleased to assemble our senior team (including practitioners) and provide further details on the issues we have identified and corrective actions we have recommended. As always, the IMA stands ready to share transformational solutions to SOX 404 implementation that protect and grow shareholder investments, allow company management to get on with the business of doing business, and restore U.S. global competitiveness for sustained long term growth.

Sincerely,



Paul A. Sharman, ACMA
President and CEO

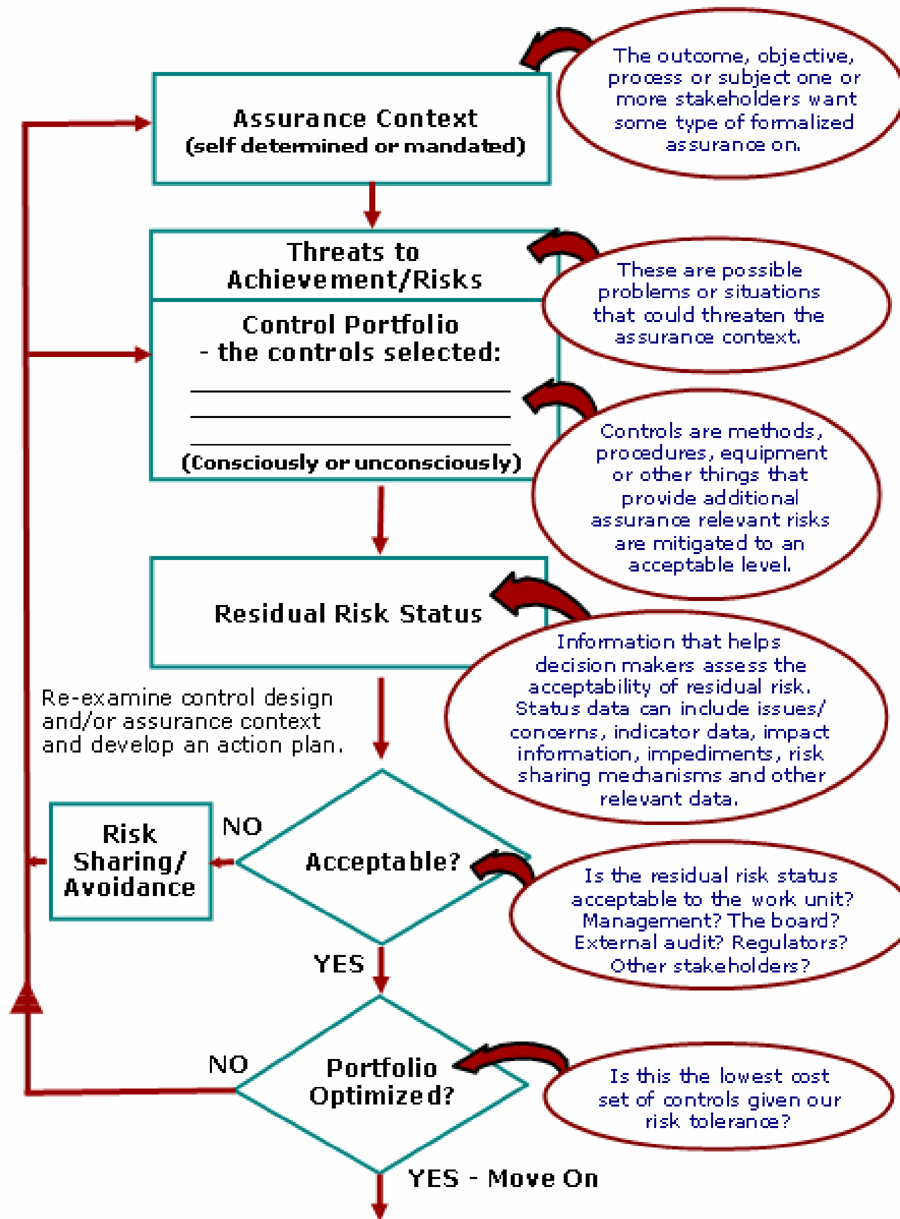


Jeffrey C. Thomson
Vice President of Research & Applications Development

INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

Attachment 1 – IMA Global Risk-Based Framework

Core Components of a Risk-Based Approach



CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

Attachment 2

IMA Technical Analysis & Commentary
SEC December 2006 Exposure Draft for Comment
Management's Report on Internal Control over Financial Reporting

Organized in ascending page order – IMA selected topic headings

PRIMARY AIM OF THE INTERPRETATION

SEC Draft Guidance:

Page 1 SUMMARY section states "The interpretive guidance sets forth an approach by which management can conduct a top-down, risk-based evaluation of internal control over financial reporting".

IMA Analysis/Comment:

With respect, this draft does not accomplish that aim, at least in terms of methods and terminology generally used and understood in risk management.

The words "top-down/risk-based" have been used frequently in guidance issued by the SEC and PCAOB over the past 3 years. A major problem appears to be definitional – what do the SEC authors actually mean by the term "top-down/risk-based"? What is clear from a detailed analysis of the document is that when the term "top-down/risk-based" is used, it is not consistent with globally accepted risk management assessment methods or standards, or in the sense described in the 2004 COSO ERM framework.

Although there are no references anywhere in the guidance that discloses the source of the SEC/PCAOB interpretation of the term "top-down/risk-based", the evidence suggests that the term has been interpreted primarily drawing from traditional U.S. audit literature and guidance issued over the past 30 years. If a guess was to be ventured as to the primary interpretation source, it appears to most closely align with notions espoused in how to evaluate "audit risk", the risk of giving an incorrect audit opinion, and the type of steps that should be done during the audit planning phase. Auditing methodologies in use today have not in any significant way adopted internationally accepted approaches to risk management, approaches that focus heavily on determining risk likelihood and consequence, and careful, formal monitoring of the status and acceptability of residual risk. Litigation risk related to adopting a true risk management approach to audits may be at the root of the non-adoption of true risk management methods.

CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

The IMA discussion paper filed in September 2006 in response to the SEC Concept Release proposes a specific market-tested, risk-based ICFR assessment approach that is scalable for organizations of all sizes. An extract from that document that describes the core elements of a risk-based approach that is aligned with global risk management standards appears as Attachment 1 of the primary IMA comment letter this detailed analysis supports.

SEC ON FLEXIBILITY ALLOWED

SEC Draft Guidance:

On page 4 it states "Instead of providing specific guidance regarding the evaluation, we expressed our belief that the methods of conducting the evaluation of ICFR will, and should, vary from company to company and will depend on the circumstances of the company and significance of the controls. We continue to believe that it is impractical to prescribe a single methodology that meets the needs of every company....Management must bring its own experience and informed judgment to bear in order to design an evaluation process that meets the needs of its company and provides reasonable assurance for its assessment. This proposed guidance is intended to allow management flexibility to design such an evaluation process."

IMA Analysis/Comment:

While the intent of this declaration to allow extensive flexibility and judgment is good, the reality is that, under the current SEC/PCAOB rules, it is the external auditor who decides whether a company's ICFR gets a "passing grade". As a result, the level of flexibility offered by either the current or proposed SEC rules is significantly undermined by the fact that management teams that want a pass on ICFR from their auditors must conform to the more granular and prescriptive PCAOB rules.

SUITABLE ICFR EVALUATION FRAMEWORK

SEC Draft Guidance:

On page 5 it states "In order to facilitate the comparability of the assessment reports among companies, our rules implementing Section 404 require management to base its assessment of a company's internal control on a suitable evaluation framework. ....the Commission identified the Internal Control-Integrated Framework created by the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") as an example of a suitable framework". The SEC's Advisory Committee On Smaller Public Companies (SPCs) contradicted the SEC stated view that COSO 1992 is suitable, at least for smaller public companies, when they stated "unless and until a framework for assessing internal control over financial reporting is developed that recognizes their characteristics and needs" they requested an exemption from Section 404.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

As far as we are aware, subsequent to the release of the COSO SPC guidance in final in June 2006, the conclusion of the Advisory Committee members on the existence of a suitable assessment framework for SPCs has not changed.

IMA Analysis/Comment:

The IMA research report "COSO 1992 Control Framework and Management Reporting on Internal Control Survey and Analysis of Implementation Practice" concluded that COSO 1992 was not designed to meet, nor does it satisfy in a demonstrable way, the "suitability" criteria defined by the SEC. Those suitability criteria are consistent quantitative/qualitative conclusions, absence of bias, comprehensive coverage, and suitability for ICFR. The IMA is a founding member of COSO and has identified the "suitability" for SOX issue to the other members of COSO. Other companies and individuals that have responded to the SEC and PCAOB have also concluded that COSO 1992 is not suitable in isolation as a primary framework to conduct ICFR assessments for SOX.

Other countries around the world, including Canada, the UK and Japan, through their actions, have similarly concluded that existing tools and frameworks are not sufficiently advanced to support the requirements for management and auditor reporting on ICFR defined by the SEC. An FEI research study completed in 2005 on material weakness deficiency reporting also identified the fact that few, if any, registrants were reporting control deficiencies and specifically identifying the relevant COSO framework category or criteria that links to the material weakness or significant deficiency identified. It is important to note that nowhere in PCAOB AS 2 does it define specific audit steps to evaluate a management claim that their ICFR controls are effective in accordance with COSO 1992 or any other control framework. To date, there has been no official acknowledgement of the growing body of evidence, including the rigorous IMA research study, that refutes that COSO 1992 actually meets the specific assessment framework suitability criteria defined by the SEC.

WHO DECIDES WHETHER CONTROL IS "EFFECTIVE" OR NOT?

SEC Draft Guidance:

On page 8 it states "In response to this feedback, the Commission and its staff issued guidance on May 16, 2005, emphasizing that management, not the auditor, is responsible for determining the appropriate nature and form of internal controls for the company as well as their evaluation methods and procedures". On page 10 it states with respect to U.S. Government Accountability Office report "That report stated that management's implementation and evaluation efforts were largely driven by AS No. 2 because guidance was not available for management."

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

IMA Analysis/Comment:

The intent of the May 16, 2005 SEC guidance is commendable. However, the reality is, under the current rules, auditors are responsible for providing an independent, subjective, parallel opinion on control "effectiveness", as well as an opinion on management's assessment. The new draft SEC and PCAOB rules recommend that the audit opinion on management's assessment be dropped, but the subjective, parallel direct report audit opinion on ICFR retained. This means that, in reality, if the approach used by management does not fully conform to the assessment approach prescribed in PCAOB AS 2, there is a significant risk that the auditor will arrive at a conclusion on control effectiveness which differs from that of management. IMA research clearly indicates the vast majority of companies used PCAOB AS 2 during the first three reporting periods as their primary assessment guidance. We are not aware of a single company in the world that attempted to complete their ICFR assessment using SEC guidance and COSO 1992 in isolation of the granular and prescriptive requirements in PCAOB AS2. The potential that parallel, but different, "how to" ICFR assessment guidance will produce unnecessary complexity and confusion has been identified as a major issue in the main body of our comment letter.

MANAGEMENT SHOULD USE ITS OWN EXPERIENCE AND JUDGMENT

SEC Draft Guidance:

On page 14 it states "Management should use its own experience and informed judgment in designing an evaluation process that aligns with the operations, financial reporting risks and processes of the company".

IMA Analysis/Comment:

Again, although this is good in theory, the reality is quite different. Management teams that want to minimize ICFR opinion variation risk will base their assessment and evaluation on PCAOB rules and the particular views on what controls must be in place.

MANAGEMENT FLEXIBILITY REEMPHASIZED

SEC Draft Guidance:

Pages 15 and 16 repeat the contention that management has significant latitude in deciding how to go about assessing and reporting on ICFR and states the approach should be "top-down, risk-based that allows for exercise of significant judgment so that management can design and conduct an evaluation that is tailored to its company's individual circumstances."

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

It goes on to state "This guidance describes a top-down, risk-based approach to this principle, including the role of entity level controls in assessing financial reporting risks and the adequacy of controls."

IMA Analysis/Comment:

We reiterate that flexibility is, in reality, limited to whether management has followed the same steps their auditors will apply in arriving at their parallel, independent and subjective opinion on ICFR. Although the words "top-down, risk-based" are used, it does not state that the exercise should start by identifying and assessing the major risks that are already known to have resulted in materially wrong financial statements and specifically linking the controls in place in the company to mitigate those risks. Informal polls conducted in locations in the U.S. and other countries around the world with SEC registrants confirm that only a very few companies during the first two reporting cycles actually listed major risks at the entity level and specifically identified what controls, if any, were in place to mitigate them. This methodology deficiency was done with the full knowledge and support of their external audit firms on the basis that the current SEC and PCAOB rules do not require this step be done by either management or auditors. It is not clear that the new draft guidance corrects this major deficiency.

IDENTIFYING FINANCIAL REPORTING RISKS AND CONTROLS

SEC Draft Guidance:

Page 21 states "The evaluation begins with identification and assessment of the risks to reliable financial reporting (i.e. materially accurate financial statements), including changes in those risks." What is missing in the current draft guidance is any form of tangible guidance how this step should be done at the entity level, subsidiary level, and account/note levels. On page 23 it goes on to state "Management uses its knowledge and understanding of the business, its organization, operations and processes to consider the source and potential likelihood of misstatements in financial statement elements and identifies those that could result in a material misstatement to the financial statements."

IMA Analysis/Comment:

The importance of the entity level risk identification and assessment step, combined with the high frequency this step was not done by either management teams or auditors in many of the ICFR assessments performed to date, suggests that there is a still a major void in the draft SEC and PCAOB guidance. Risk management specialists have recognized that the experiential/brainstorming approach to risk identification that draws solely on participant experience and knowledge, in isolation, regularly produces seriously deficient lists of significant risks.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Given that the dominant entity-level risk in the major scandals to date, including Enron, WorldCom, HealthSouth, Parmalat, Nortel and many others has been "CEO/CFO direct inappropriate accounting entries be booked", it would seem to make sense that regulators offer this as a specific example of a real-life, high probability/high impact risk. Other examples of significant entity level risks include "CFO/Controller not current on technical GAAP reporting rules", "CFO/Controller not technically current and up to date on all applicable tax rules", etc.

The SEC should, without too much work, be able to provide a list of the top ten statistically probable risks that have resulted in materially wrong financial statements. The guidance could then indicate that, at a minimum, these known statistically probable high consequence risks should be identified, assessed for applicability in the specific business sector, and documented as entity level risks. It isn't clear why the guidance appears to go to some lengths avoiding simply stating that statistically probable risks should be documented, likelihood/consequence assigned, and the controls in place, if any, that mitigate the risk identified and evaluated. There is no real guidance offered in the current exposure drafts on how this critically important step should be done, other than referencing management experience, a method which is globally known, if used in isolation, to produce incomplete risk assessments in a significant number of cases.

Some of the globally accepted methods to ensure the completeness and reliability of the risk identification step outlined in the September 15, 2006 IMA discussion paper "A Global Perspective on Assessing ICFR" filed with the SEC include the following:

1. **Loss/Incident Approach** – This uses internal error tracking to identify relevant risk or risks that were key to control failures that have been detected by management, internal and external auditors and others. This is now a mandatory step required by the Basel II reforms for all banks around the world. In practice this would mean systematically creating 3 to 5 years of situations where errors were identified in draft financial statements by the compay's auditors – both material and immaterial. These "defects" are analyzed for patterns and trends and root cause and correlated factors identified. There is a huge body of experience globally emerging how to execute this critical risk-based step. The quality movement has an impressive body of knowledge on how defect analysis is key to process improvement.

2**. Risk Source Approach** – This method uses a "risk source" framework that helps the people doing the assessment to ensure they have considered all the key risk sources and evaluated applicability to their circumstances. Examples of risk sources include such things as suppliers, technology, employees, human behavior, customers, economics, contractual, regulators, and others. The September 15, 2006 IMA Discussion Paper "A Global Perspective on Assessing ICFR" provides specific illustrations of a risk source framework. Attachment 1 to this comment letter provides a process summary of IMA's risk-based framework.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

3. **Inverse Control Approach** – This method focuses on risks that flow from the non-use of particular controls. An example in accounting would be "employees lack the necessary knowledge/skill" or "employees have not completed a reliable risk assessment". Control frameworks like COSO and CoCo in Canada identify capability controls as part of an integrated framework. The absence of a particular type of control may be a risk. An example of an inverse control approach in the home environment related to fire safety would be "No smoke detectors are installed". The real root risk is that a fire in the house has started but occupants are not aware of it.

4. **Brainstorming/Experiential Approach** – This approach is unstructured and draws on the experience and knowledge of participants. The broader and more complete the experience the better the list of risks that have already happened. The approach when used in isolation has a high failure rate in terms of producing reliable lists of all significant risks.

5. **Visualization/process mapping** – This approach requires participants to formally trace the steps involved in an activity/process and to use that knowledge to identify points or steps that may involve risks. This is a very time/labor intensive method but can yield good results.

6. **External Research** – This approach draws on identifying what has already been learned about risks and risk vulnerability in a particular business sector or activity. Vendors such as Audit Analytics and Compliance Week provide detailed tracking of material weakness disclosures of all U.S. listed companies. Problems that impact on more than a few companies in a specific business sector should be specifically examined for applicability in others. Again, the Basel II reforms for banking have made external benchmarking a mandatory risk management process for all major banks around the world.

WHAT DOES "ADEQUATELY ADDRESS" MEAN?

SEC Draft Guidance:

On page 25 the guidance states "the objective of this evaluation step is to identify controls that adequately address the risk of misstatement for the financial statement element that result in a material misstatement in the financial statements."

IMA Analysis/Comment:

Although the statements in this section are technically correct they could be stated in a clearer way and better convey just how difficult this step is in practice. An example to illustrate the challenge follows:

Risk: The CFO directs improper entries to manage period profits in order to maximize personal gains under the company's stock option/bonus system. Risk likelihood rating – low (over the entire population of public companies but not necessarily in specific companies); Risk consequences rating – severe.

Mitigating Controls:

1. Audit committee reviews financial statements prior to release.
2. Company maintains a concerns reporting hotline that is reviewed and responded to by internal audit.
3. Company has a code of conduct that stresses the obligation of the company to report reliable financial statements.
4. Internal audit department completes an audit of the financial statement close process on a 3 year cycle.

Extending this example to the "residual risk" step a hypothetical residual risk status for a sample company could be as follows:

External auditors identified 3 to 6 material errors in the draft financial statements prepared under the direction of the CFO in each of the previous four fiscal periods. These errors had to be corrected prior to the auditors signing the financial statements. 30% of the errors identified by the auditors were attributed to controllership GAAP knowledge/skill deficiencies, 30% were attributed to flawed transaction processing control design at the subsidiary level, and 40% were attributed to conscious acts and decisions on the part of senior management to manage profit to meet earning forecasts through selective and, at least in the opinion of the company's auditors, inappropriate interpretation and application of GAAP rules. No process is currently used by management or auditors to document, track, and analyze errors detected over time. Management has regularly reported in response to a range of internal audit findings that they are prepared to accept the risk. Few, if any, external audit firms have formal IT systems in place that systematically log and analyze cause of accounting errors detected during the substantive audit phase of the audit over multiple fiscal years.

It is important to note that neither the SEC or PCAOB current or draft guidance indicates that there is any requirement for management or auditors to formally document and monitor residual risk status. Residual risk is a key element of virtually all generally accepted risk management standards in use around the world.

In practice, the ICFR controls in place always result in some level of residual risk which is more or less acceptable to any given combination of stakeholders. The "RISK-BASED" illustration above would be a fairly common status description, especially in non-accelerated filers. In many cases, subjective views by management and/or auditors on whether a given combination of controls will produce the desired results are proven by the passage of time to be wrong.

There is at least preliminary evidence that many of the companies that are under investigation for accounting errors related to stock option accounting have CEOs and CFOs who have regularly certified that the company has effective disclosure and ICFR controls and at least some received "effective" control ratings from their auditors prior to the disclosure of the problem. Monitoring of changes in residual risk status, including detected error rates found by external audit and management,

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

reduces the enormous subjectivity in the vast majority of ICFR assessment methods in use today for SOX.

IT GENERAL CONTROLS AND RISK

SEC Draft Guidance:

On pages 27 and 28 there is a discussion of the role of IT general controls and it states on page 28 "For purposes of evaluation of ICFR, management only needs to evaluate those general IT controls that are necessary to adequately address financial reporting risks."

IMA Analysis/Comment:

Although there is a general reference to risk and risk-based, the reality is that IT general controls in the context of SOX should be defined as controls in place to address a specific class of risks that do, or could potentially, threaten the reliability of the financial statements. Relevant IT general controls risks include "Fraudulent modification of program code", "Unauthorized modification of data used in the calculation/preparation of accounting entries", and "Logic and/or calculations performed by computerized accounting systems are technically flawed and/or wrong". The main reason to evaluate what are generally known as IT General Controls is to determine if there are specific controls in place and functioning that are effective enough to mitigate the type of risk described above below a level of residual risk that is currently set in AS 2 at "less than a remote likelihood" and is proposed to be in the draft guidance less than "reasonably possible".

The guidance makes no reference to how to apply a "risk-based" approach to evaluating the effectiveness of IT general controls. In reality, a simple but radical way to test IT general controls is to have a person with strong computer skills attempt to modify key accounting programs and/or data and assess if he/she is successful and whether the controls are strong enough to detect the change. Risks in this area should include the risk that a person working in the IT department that has high level access rights attempts to make unauthorized changes to data or program code undetected. Very few companies submit their IT general controls to this level and harsh type of effectiveness evaluation. In the absence of this type of "real life risk" evaluation, conclusions arrived at as to whether controls are, or are not, effective, while still useful, are inherently subjective.

GUIDANCE DOES NOT EXPLICITELY REQUIRE RISK OR RESIDUAL RISK INFORMATION BE DOCUMENTED

SEC Draft Guidance:

On page 28 it outlines documentation requirements and states that "management must maintain reasonable support for its assessment". Nowhere in this section does it explicitly state that management needs to document relevant risks to reliable financial statements at the entity, subsidiary or account/note levels, or maintain any

documentation related to management's assessment of the likelihood or consequence of the risks identified.

Considerable attention is paid in the draft guidance to the need to document controls. The words "risk characteristics" are used but there is no direct requirement to document risks that threaten the reliability of the accounts at the entity or subsidiary levels. It goes on to state on page 30 "Evidence about the effective operation of controls may be obtained from direct testing of controls and on-going monitoring activities".

IMA Analysis/Comment:

Although there is a reference to "monitoring activities" nowhere does it state that management needs to determine the current actual detected error rate related to specific accounting line items or note disclosures in the company's draft financial statements. Control evaluation in the total absence of a focus on the actual error or defect rate is inherently subjective. Current ICFR assessment methods in use during the first three rounds of SOX reporting have shown a high effectiveness conclusion failure rate.

The IIA in its guidance on issuing audit opinions indicates that auditors should be very cautious issuing pass/fail audit opinions in areas where the assessment criteria are open to wide interpretation by knowledgeable experts. A Glass & Lewis study clearly indicated that literally thousands of companies reported having effective ICFR controls right up to the time of their first 404(b) audit report under effective disclosure reporting rules. At that time the auditors determined during their audit that there were material errors in the financial statements that required correction.

Under the current PCAOB rules detection of a material error in the draft statements generally forces management to indicate ICFR controls are ineffective and disclose one or more material weaknesses. It is assumed that in the hundreds of cases identified in the Glass & Lewis research study neither management or auditors had concluded based on their ICFR assessment prior to the time the financial statement defects were found that there were any reportable control deficiencies.

DETERMINING THE SUFFICIENCY OF EVIDENCE

SEC Draft Guidance:

The diagram on page 32 provides a useful guide in terms of where the most persuasive evidence should be obtained by management. It uses the term "misstatement risk of financial reporting element". Presumably this diagram can apply to the whole of the financial statement filings with the SEC or specific accounts and notes. The x axis is labeled "risk of control failure". If this table was applied to the very real risk that the CEO and CFO often, if not always, have significant financial incentives to manage and/or manipulate profit, it would suggest this risk should be scored as a top right quadrant risk. The controls to manage this very real and

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

significant risk include the audit committee diligence and competency, confidential concerns hotlines, likelihood and severity of sanctions if caught, and others.

Although SEC ICFR rules do not allow it to be counted in control assessment work or evaluated as to its sufficiency, in reality, the highest impact control to mitigate this specific risk is the ethics and competency of the specific external audit team assigned to audit the financial statements prepared by management.

IMA Analysis/Comment:

This table is, in fact, at the root of a significant amount of inefficient work done to date. The table correctly suggests that the most evidence should be obtained on the controls in place to manage the really serious, statistically probable, entity-level risks that are already known to have been at the root of major financial scandals and auditor opinion failures. It is not a stretch to conclude that this means that the most persuasive evidence should be gathered on the diligence and competency of the audit committee, and the competency, ethics, and quality assurance controls of the company's external audit firm.

Research done by FEI on control deficiency reporting during 2004 and 2005 indicates that either 1) virtually all audit committees of U.S. public companies are "effective" as key controls, or 2) explicit SEC and PCAOB requirements to complete this step and sound risk management principles that call for the most rigorous assessment and most persuasive evidence should be gathered on the truly key controls are not being complied with. Given numerous studies undertaken around the world over the past 20 years cast serious doubt on the 100% effective audit committee option, the evidence points to the conclusion that audit committees are not being rigorously assessed in terms of their role as a key control. The reason is simple - it is too dangerous from a career perspective for insiders to complete the step in a rigorous way and it requires external auditors evaluate the very people that have hired them – the audit committee.

In the case of evaluating the likely effectiveness of the external auditor as a control, the current rules do not allow this form of assessment to be completed or counted in SOX reviews. Because it is the external auditor that is currently being asked to form an independent subjective view on management's controls, this would also mean that the external audit would be required to report on management's assessment of their own competency, ethics and quality assurance system. This of course would be a major conflict of interest and under the current rules is impossible to complete as a step for a variety of reasons. This point means that by definition, the current rules do not adequately address, at least in a true risk-based way, one of the most significant risks that have lead to major financial misstatements – senior executive directed financial statement fraud.

ASSESSING CONTROL EFFECTIVENESS – SUBJECTIVE/OPINION-BASED VS FACT-BASED ASSESSMENT

SEC Draft Guidance:

On pages 35-38 there is considerable discussion of examining the operation of controls but very little discussion of evaluating and measuring risks as a key precondition to deciding on the likely effectiveness of the current control design and operation. The words "residual risk" are not used anywhere during this discussion. A key element of residual risk is the current "defect or error rate" or, stated another way, the frequency and magnitude detected where the controls in use did not result in reliable financial statements.

IMA Analysis/Comment:

In any true risk-based approach the process starts by identifying and assessing risks that threaten the specific "assurance context" being evaluated. For SOX, the macro assurance context is that the financial statements at the consolidated entity level are reliable. This must then be cascaded down to account and note level at the consolidated level and on down to the entity level at significant subsidiaries, if any, that make up the consolidated statements. Only after this step is completed should the controls, or "risk treatment" mechanisms in risk management vernacular, be identified. Once controls in place have been identified and tested to confirm a correct understanding of the risk mitigation strategy it is essential to then take steps to determine the residual risk status. Residual risks are risks that remain after considering the risk treatment steps taken.

For ICFR this is comprised of risks where there were either no controls identified or the controls are not expected to fully mitigate the risk(s) identified in whole or part, as well as the current performance level and error rate being produced by the controls in place. In the case of ICFR, this is comprised of errors, both large and small, detected by external auditors during their audit, errors detected by management both before and after public release of the statements, errors detected by tax authorities and others after financial statements are released, results of comparisons of management estimates made to actual results that occurred in subsequent periods, and other key information.

This approach to evaluating control effectiveness is considered to be "fact-based" as opposed to approaches that are primarily "subjective/opinion-based". Unfortunately, under the current rules, the vast majority of ICFR assessments being done currently are regulator endorsed subjective/opinion-based. One way to get a sense of the current failure rate of ICFR assessment methods currently in use is to measure the frequency that both management and auditors conclude ICFR control for a specific account or note disclosure is "effective" during their ICFR assessment, versus the frequency that auditors identify material defects in the accounts and notes during their audit of the financial statements provided by management.

Research conducted by the FEI and Glass & Lewis indicates that current subjective/opinion-based ICFR assessment methods have a relatively high failure rate. Limited research, if any, is being done to carefully and systematically identify and track management or auditor ICFR effectiveness prediction accuracy.

EVIDENTIAL MATTER TO SUPPORT THE ASSESSMENT

SEC Draft Guidance:

Pages 38 and 39 outline the evidential matter necessary to support a conclusion.

IMA Analysis/Comment:

Although flexibility in the required assessment approach is a positive attribute from a management perspective, this section, in light of the considerably more granular requirements in the PCAOB standard, provides limited practical help. If management does not approach the ICFR assessment in the same way required by the PCAOB standard the possibility of a control effectiveness conclusion different than that arrived at the company's external auditor increases. The guidance would be greatly improved if it simply stated minimum expectations at the entity, account, note and subsidiary levels. A table for this purpose would be a much better vehicle to communicate this information. It should be possible for the authors to simply review each of the "how-to" sections in the guide and summarize the minimum data that is expected to be assembled. There is no indication that there is any expectation that fact-based residual risk/ICFR system performance data should be obtained and stored on file to provide fact-based conclusions on ICFR effectiveness.

MATERIAL WEAKNESS EVALUATION

SEC Draft Guidance:

Pages 41 to 46 discuss how to grade control deficiencies including specific guidance on what constitutes "strong indicators" of a material weakness.

IMA Analysis/Comment:

While this guidance is a major improvement over what was previously available for management, it still misses a key point that is relevant to users of the information. Research done by the FEI and Glass & Lewis indicates a considerable number of the material weaknesses are being disclosed as a result of auditors finding material errors in drafts prepared by management. This situation is classed as a strong indicator of a material weakness. The list on page 45 includes the following strong indicator:

Identification by the auditor of a material weakness in financial statements in the current period under circumstances that indicate the misstatement would not have been discovered by the company's ICFR.

A simple way of expressing where the draft financial statement quality bar is currently set is to simply indicate that "The ICFR controls in place must be capable of preventing a material error in the draft financial statements provided to the company's external auditors. If your assessment indicates that there is at least a reasonable possibility that a material error will be present in the draft financial statements provided to the auditors, the situation must be identified and reported as a material weakness."

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

The issue of where the draft financial statement quality bar is set for all companies currently is identified as a major issue in the main body of the IMA comment letter. The current rules in use and those contained in the SEC and PCAOB exposure drafts require management produce draft financial statements with zero material defects or face the consequences that flow from publicly reporting that the company has an ineffective ICFR system. This is a quality level that is far beyond that in any other country in the world today and a far more stringent level of internal financial reporting quality than is currently being produced by the majority of smaller public companies. The fact that current and proposed SEC and PCAOB rules require zero material defects in financial statement draft or be labeled as having an ineffective ICFR system will, in all probability, continue to fuel objections from U.S. SPCs, and add fuel to the movement to de-list and/or list securities in countries with lower draft financial statement quality requirements (i.e. lower than zero material defects). At this point there is no empirical research that examines whether the current U.S. rule of zero material defect in draft financial statements or publicly disclose an ineffective ICFR system produces a higher audit opinion reliability rate than that in other countries.

PROPOSED RULE AMENDMENTS

SEC Draft Guidance:

On page 51 it states "an evaluation conducted in accordance with the interpretative guidance issued by the Commission, if the Commission adopts the interpretative guidance in final form, would satisfy the annual management evaluation required by those rules. The proposed amendments would not limit the ability of management to use its judgment to determine the method of evaluation that is appropriate for its company. The proposed amendments would be similar to a non-exclusive safe-harbor in that they would not require management to conduct the evaluation in accordance with the interpretative guidance, but would provide certainty to management that choose to follow the guidance that it has satisfied its obligation to conduct an evaluation for purposes of the requirements in Rules 13a-15(c) and 15d to-15(c)."

IMA Analysis/Comment:

Given that the proposed guidance calls for the auditors to do a separate and independent assessment of ICFR following the procedures in the new PCAOB standard, it would appear to make little practical sense for management to do their analysis in accordance with any rules other than the assessment rules the auditor must follow. We are very concerned that this situation may make the entire SEC document largely redundant. This point is identified as a major issue in the main body of IMA's comment letter.

INDEPENDENT AUDITOR OPINION ON ICFR

SEC Draft Guidance:

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

On page 52 it states "Therefore, we are proposing to revise Rule 2-02(f) to require the auditor to express an opinion directly on the effectiveness of ICFR".

IMA Analysis/Comment:

There is no discussion in the draft of the significant groups, including the IMA and IIA and small accelerated filers (e.g., Alamo Group response letter January 3, 2007), that have publicly disagreed with the SEC's interpretation of section 404(b). IMA research indicates that current ICFR assessment frameworks are inherently subjective and that no control frameworks currently available meets the four specific suitability criteria defined by the SEC. The SEC's own SPC advisory board indicated "unless and until a framework for assessing control over financial reporting for such companies is developed that recognizes their characteristics and needs, provide exemptive relief from Section 404 requirements of the Sarbanes-Oxley Act". The SEC position that the Act calls for a subjective and public opinion from external auditors on whether a company's ICFR framework should be assigned a pass/fail rating amplifies the negative impacts flowing from the current rules. This issue is identified in the IMA primary response letter this detailed analysis supports as a major issue.

SIGNIFICANT ALTERNATIVES

SEC Draft Guidance:

On page 64 it indicates that "The Regulatory Flexibility Act directs us to consider alternatives that would accomplish stated objectives, while minimizing any significant adverse impact on small entities."

IMA Analysis/Comment:

There is no evidence at this point that the SEC has considered in any serious way two major alternatives that are open to it.

These are:

1. Actually allow and encourage companies to use globally accepted risk management assessment methods such as those outlined in international risk standards, COSO ERM and the discussion paper the IMA filed with the SEC in September to meet the requirements of Section 404 (see Attachment 1 to this comment letter for a process summary of IMA's risk-based framework). Such an approach would focus on entity level risk identification and assessment and residual risk monitoring to significantly greater extent than the current SEC/PCAOB control-centric rules. This type of approach would require "fact-based" evaluation of control effectiveness as opposed to current criteria which are predominantly subjective, particularly as they relate to analysis of "entity-level controls", fraud prevention/detection controls and IT general controls.

2. Require that auditors provide an opinion on the reliability of management's assessment process drawing on well developed and accepted process auditing

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

methodology used in the quality profession instead of the current path of requiring a subjective, independent auditor opinion on ICFR using different assessment guidance than that offered to management.

It is not clear why these alternative approaches have been rejected as no explanation for rejecting them has been offered to date.

REFERENCES

1. "A Global Perspective On Assessing Internal Control Over Financial Reporting, Discussion Draft for Comment", Institute of Management Accountants, September 2006.
2. "COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices", Parveen P. Gupta, LLB, Ph.D., Institute of Management Accountants, 2006.
3. "Enterprise Risk Management: Frameworks, Elements and Integration", William Shenkir, Ph.D, CPA and Paul Walker, Ph.D., CPA, Institute of Management Accountants, 2006.
4. "Control Deficiency Reporting: Review and Analysis of Filings During 2004", Parveen Gupta, L.L.B., Ph.D, Tim Leech , FCA·CIA·IT, CCSA, CFE, Financial Executives Research Foundation, 2005.
5. "Final Report of the Advisory Committee on Smaller Public Companies to the United States Securities and Exchange Commission", Herbert S. Wander and James C. Thyer Committee Co-Chairs, April 23, 2006.
6. "Sarbanes-Oxley: A Practical Guide to Implementation Challenges and Global Response", Sally Chan CMA, ACIS, Parveen Gupta L.L.B, Ph.D., Tim Leech FCA·CIA·IT, CCSA, CFE. 2006.
7. "Control Deficiencies – Finding Financial Statement Impurities: Analysis of the 2004 and Early 2005 Deficiency Disclosures", Glass, Lewis and Co. LLC, June 2005.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Attachment 3

IMA Technical Analysis and Commentary
PCAOB RELEASE No. 2006-007 (ASX/5) 12/19/06

Organized in ascending page order – IMA selected topic headings

PROCESS EFFICIENCY

PCAOB Draft Standard:

Page 3 states "the Board has evaluated every significant aspect of the audit of internal control to determine whether the existing standard encourages auditors to perform procedures that are not necessary in order to achieve the intended benefits".

IMA Analysis/Comment:

We appreciate the paragraphs in the draft standard that are devoted to explaining the position taken on whether the Act calls for an audit of management's ICFR assessment versus an independent and subjective audit opinion on ICFR. However, there is no indication that the PCAOB or SEC have examined the impact of their choice on the overall cost of compliance. There is also limited indication that the PCAOB has formally considered what a "top-down/risk-based" ICFR approach would look like based on globally accepted risk management standards such as those in AS/NZ 4360 or COSO ERM.

GENERAL IMPROVEMENTS TO THE STANDARD

PCAOB Draft Standard:

Page 4 states that the proposals are designed primarily to:

Focus the audit on the matters most important to internal control
Eliminate unnecessary procedures
Scale the audit for smaller companies
Simplify the requirements

IMA Analysis/Comment:

To achieve these laudable goals, IMA suggests that the current draft be changed to require that management and auditors identify, document and assess the statistically probable macro level risks that are already known to be the cause of materially wrong financial statements. If the goal is to eliminate unnecessary procedures it would seem reasonable to focus on the highest likelihood/biggest consequence risks to unreliable accounts and notes.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

If the draft standard is intended to scale for smaller companies one can question why this revision retained a standard that requires management produce draft financial statements with zero material defects or face having to report they have ineffective controls over financial reporting overall. If a key goal is to simplify the requirements one has to question why the draft standard does not simply direct auditors to use the same "how to guidance" management must use to assess and report on ICFR.

PCAOB ON TOP-DOWN

PCAOB Draft Standard:

Page 5 states "When using a top-down approach, the auditor identifies the controls to test by starting at the top – the financial statement and company-level controls – and linking the financial statement elements and company-level controls to significant accounts, relevant assertions, and, finally, to the significant processes where other important controls reside. Following the top-down approach helps the auditor focus the testing on the right controls – those controls that are important to the auditor's conclusion – while avoiding those that are outside of the scope of the audit of internal control. In a top-down approach, if company-level controls are strong and link directly to process-level controls, or if they are sufficiently precise to prevent or detect material misstatements to relevant assertions, the auditor **will likely** be able to reduce the testing of controls at the process level."

IMA Analysis/Comment:

This paragraph is indicative of a fundamental problem in the guidance – it is not, in reality, risk-based or top-down by globally accepted risk management standards. Nowhere in the words above does it say the auditor should start by identifying the high level risks that are already known to be the major causes of major financial statement errors in U.S. listed companies and then, only after that step is done, identify the high level controls in place, if any, to mitigate them. Without first identifying and documenting entity level risks, any attempts to document company level controls will be less focused and efficient than it could be. Key entity level risks include CEO/CFO directed manipulation of earnings, CFO/controller staff not current/knowledgeable on GAAP treatment, a senior management reward system that offers massive incentives to falsify earnings, CFO/controllership knowledge of applicable tax rules, etc.

PCAOB ON RISK-BASED

PCAOB Draft Standard:

Page 7 states "The proposed standard on auditing internal control, therefore, requires risk assessment at each of the decision points in a top-down approach. The auditor's identification of significant accounts and relevant assertions requires an understanding of the related risks and how those risks should affect the auditor's decision making.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Importantly, the proposed standard makes clear that the evidence necessary to persuade the auditor that a control is effective depends on the risk associated with the control."

IMA Analysis/Comment:

Although this paragraph admirably gives credence to the notion of "risk-based" assessment, it doesn't actually say that the auditor should either evaluate the completeness of the risks identified and documented by management. Nor does it indicate that the auditors themselves **must** identify and document relevant risks together with their assumptions regarding the likelihood and consequence of those risks and then document and test the specific controls in place, if any, to mitigate the risks identified.

PCAOB ON RISK TOLERANCE

PCAOB Draft Standard:

Page 12 states "Sometimes, however, the auditor may find that the company evaluated the significant deficiencies and reasonably determined under the circumstances not to correct them. When that is the case, the proposed standard would allow the auditor to conclude the control environment is effective and that no material weakness exists."

IMA Analysis/Comment:

In smaller public companies this comment begs the question "What if the deficiency is that the accounting staff lack the technical knowledge or skill to properly account for the transaction and management is fully aware of this deficiency and has previously relied on their external auditor to compensate?" An analogy would be a GP doctor that recognizes he or she is not qualified for brain surgery and refers their patient to a specialist. Many small and even large companies identify areas and transactions that they don't feel confident dealing with to their external auditor. The auditors source the necessary expertise to provide direct assistance up to, and including, identifying the necessary accounting entries to handle the transaction properly. If this paragraph is taken literally, what does the auditor do when there are dozens of risk acceptance decisions that have been made and communicated to him/her by management where management knows and candidly acknowledge that their controls in certain defined areas will not prevent a material error in their draft statements?

PCAOB ON ELIMINATING "UNNECESSARY" PROCEDURES

PCAOB Draft Standard:

Page 14 states **"the proposals would eliminate the requirement to evaluate the process management used to evaluate its internal control"**.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Page 16 states "The Board also believes that the auditor can perform an effective audit of internal control without conducting an evaluation of the adequacy of management's evaluation process." On page 17 it states "The proposal eliminates the opinion on internal control on management's assessment because it is redundant of the opinion internal control itself and because the latter opinion more clearly conveys the same information – specifically, whether the company's internal control is effective."

IMA Analysis/Comment:

The Act states in section 404(b) that "each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer." It is a question of law whether the SEC and/or PCAOB have the legislative authority to eliminate a step called for by the law on the basis it is "an unnecessary procedure". The issue of regulatory authority is outside the scope of this comment paper. What is relevant is that the paragraph on page 15 of the draft standard does not acknowledge that a growing number of practitioners, including those represented by the IMA and IIA (nearly 200,000 members combined) have questioned whether the Act intended that auditors provide an independent and subjective opinion on ICFR.

From a technical standpoint it is difficult to understand how sound and fully defensible decisions on how much to rely on management's ICFR work can be made without doing a reasonably thorough evaluation of whether management's work can and should be trusted. The draft standard recognizes this when it states on page 16 ***"Although the removal of the evaluation requirement should eliminate unnecessary work, the quality of management's process is inherently linked to the amount of work the auditor will need to do. For example, the extent of the auditor's ability to use the work of others will depend on the quality of the company's annual evaluation process and its ongoing monitoring activities, as well as on the competence and objectivity of those performing the work. For this reason, it will continue to be necessary for the auditor and management to coordinate their respective efforts."*** One must assume that the PCAOB has decided "coordinate" is quite different from completing audit work to determine if management's work is reliable and should be relied on. Later in the draft it goes on to emphasize the importance of auditors relying on management's work and calls for steps to be taken to evaluate how much reliance to place. It is fair to say that our conclusion is that the logic in this area should be revisited.

USING THE WORK OF OTHERS

PCAOB Draft Standard:

Page 22 states "the proposed standard would establish a single framework, based on the nature of the subject matter being tested and competence and objectivity of the

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

personnel performing the testing, for the auditor's decisions about using the work of others (including, but not limited to, internal auditors) as audit evidence….

The proposed standard on using the work of others first directs the auditor to **obtain an understanding of the work performed by others** to identify the activities relevant to the audit. Relevant activities are defined as those that provide evidence about design and operating effectiveness of control over financial reporting or that provide evidence about potential misstatements of the company's financial statements. …. The proposed standard would require the auditor to obtain an understanding of the work undertaken by others to determine how that work might alter the nature, timing, and extent of the work the auditor otherwise would have performed."

IMA Analysis/Comment:

It would seem that "obtaining an understanding" is quite different from evaluating and auditing management's assessment process but the distinction in this case appears questionable. It would also seem to imply that at no time does the auditor need to test whether the work product produced by management is reliable. Later the standard talks about evaluating objectivity and competence of the individual staff involved in preparing management's assessment but the draft would appear to suggest that this step can be done without actually verifying the reliability of the work produced.

SCALING THE AUDIT FOR SMALLER COMPANIES

PCAOB Draft Standard:

Page 28 states "Under the proposed standard, the auditor can use strong company level controls and **financial statement audit procedures** to reduce the level of testing for smaller companies."

IMA Analysis/Comment:

What we infer from this statement is that the auditor can count their year end audit work done as a control for purposes of ICFR assessment. This runs counter to core premises in SOX and the SEC and PCAOB standards. The current regulations do not allow management to count virtually anything done by the external auditor as an ICFR control and the AICPA recently issued guidance on that point. This statement also sets the stage for situations where, if the financial statement audit procedures are allowed to be counted as a control by the external auditor in their control evaluation, the auditors would be auditing their own work in arriving at an independent opinion on ICFR, counter to core globally accepted auditing principles.

Our experience is that smaller public companies often rely on and utilizes the expertise and knowledge of their external auditors in areas such as tax provisions, foreign exchange, consolidations, application of complex GAAP (e.g., the new rules on tax provisions), drafting of note disclosures and other difficult/complex areas.

Many smaller companies can ill-afford to retain staff or outside consultants capable of dealing with all complex elements of financial statement accounting and note disclosure.

Another problem is that there is currently an absence of generally accepted methodology to consistently and reliably evaluate company level controls. If there was a reliable entity level ICFR approach it should be capable of producing a specific and repeatable grade on company level controls (i.e., different assessors would arrive at the same conclusions independently). The grade on entity level controls should then drive specific reductions in substantive audit testing, analogous to insurance underwriting wherein the controls in place are evaluated and, subject to the result, premiums are accordingly adjusted (e.g. use of smoke detectors, driver education training for young drivers, etc.). No such reliable and repeatable entity level control evaluation system currently exists anywhere in the world that we are aware of.

SIMPLIFYING THE REQUIREMENTS

PCAOB Draft Standard:

Page 30 states "Taken as a whole, the proposals are intended to simplify the requirements and make them easier to apply while retaining the core principles necessary for an effective audit of internal control."

IMA Analysis/Comment:

While simplification is a laudable goal, the standard should be changed such that the PCAOB directs the external auditor to apply the same SEC ICFR assessment guidance management is instructed to use in arriving at their opinion on ICFR. Using this approach it should be possible to reduce the PCAOB auditing standard to 20 pages or less in length. If this was to occur and external auditors then claim that the SEC guidance is not sufficiently clear for them to arrive at an opinion on control effectiveness, how can management be expected to use the SEC ICFR guidance in isolation? Currently many specialists that have studied the December SEC and PCAOB exposure drafts agree that ASX/5 is considerably more detailed and granular than the SEC guidance for management. Given that auditor must use the PCAOB standard to arrive at their pass/fail opinion on ICFR, it is very likely that PCAOB standard will retain its position as the de facto guidance for management.

ASX TABLE OF CONTENTS – CONTROL TESTING DOMINATES; RESIDUAL RISK NOT MENTIONED AT ALL

PCAOB Draft Standard:

Page A1-2 references in the planning section the topic of "Role of Risk Assessment", however, when the steps to be applied in a Top-Down approach are listed the requirement to identify macro level risks to reliable financial disclosures is absent.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Nowhere in the draft standard is the concept of the auditor identifying and assessing residual risk status ever mentioned.

IMA Analysis/Comment:

The new guidance makes no reference to any requirement directing the auditor to identify, using a 3-5 year history, the accounts and notes that have required adjustment prior to audit sign-off to document the history and pattern of prior failures in the company's ICoFR. The draft standard does not emphasize that during the planning stage the auditor should formally analyze and document the company and industry sector's history of restatements and financial statement audit opinion errors. These steps merit being listed as stand alone content topics. When the steps to be taken for a Top-Down approach are articulated, identifying macro level risks is absent as is the requirement that the auditor take steps to identify and assess the residual risk status being produced by the current control design. This would include identifying and assessing "repair entries". Repair entries are accounting entries booked by management after a quarter or year end disclosure related to transactions or balances already publicly disclosed. This includes analysis of such things as comparing the provision for law suits against the actual settlement amounts, provision for taxes against the amounts filed and/or reassessed by tax authorities, provisions for bad debts against actual bad debt experience, etc.

THE AUDITOR'S OBJECTIVE

PCAOB Draft Standard:

Page A1-4 states "The auditor's objective in an audit of internal control over financial reporting is to express an opinion on the company's internal control over financial reporting."

IMA Analysis/Comment:

IMA respectfully believes that the SEC and PCAOB have misinterpreted the true intent of Congress in section 404 (b) of the Sarbanes-Oxley Act of 2002. The Act passed by Congress does not state that external auditors should publicly express an independent, subjective opinion on the company's ICFR. It is also important to note that, at least to the date of this analysis, no other country in the world has accepted the premise that an independent audit opinion on ICFR effectiveness is a practical and viable approach to more reliable auditor certified financial statements.

THE FRAMEWORK AUDITORS SHOULD USE

PCAOB Draft Standard:

Page A1-5 states "The auditor should use the same suitable, recognized framework to perform his or her audit of internal control over financial reporting as management uses for its annual evaluation of the effectiveness of the company's internal control over financial reporting."

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

IMA Analysis/Comment:

If the intent of this section is to direct the auditor to use the framework used by management, there should be no need for the PCAOB document to describe how auditors should complete their parallel independent ICFR assessment. Since the PCAOB has put considerably more granular detail in the draft audit standard than is currently in the SEC exposure draft, it is almost certain management will use the PCAOB guide as the primary guidance. In terms of the use of frameworks like COSO 1992, CoCo, or Cadbury, the IMA research study on the use of COSO published in 2006 provides conclusive evidence that companies have not actually been using COSO 1992 as a primary framework for SOX ICFR assessments.

PLANNING THE AUDIT

PCAOB Draft Standard:

Page A1-5/6 lists items to be covered including "knowledge of the company's internal control over financial reporting obtained during other engagements."

IMA Analysis/Comment:

This section does not explicitly require the auditor to create and analyze the pattern of mandatory audit adjustments identified during the last 3-4 audits to provide objective information on where ICFR has failed in the past. Nor does it explicitly require that the auditor obtain information on which financial statement line items and/or notes where other companies in the same business sector experienced major problems, up to and including restatements. Another omission is that the draft does not require the auditors to make inquiries and execute procedures to identify "repair entries" – entries that are correcting account balances or impact on note disclosures that have already been issued. Both types of information are relevant to fully understanding residual risk and are now widely available at a modest cost as a result of technology advances (e.g., use of software like ACL, data bases offered by Auditanalytics.com, Compliance Week and other sources).

ROLE OF RISK ASSESSMENT

PCAOB Draft Standard:

Page A1-7 states "the auditor should focus the majority of his or her attention on the areas of greatest risk to substantially decrease the opportunity for a material weakness to go undetected".

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

IMA Analysis/Comment:

Using a risk based approach derived from globally recognized risk management standards this statement should read "the auditor should focus the majority of his or her attention on the biggest risks that threaten the objective of materially reliable auditor certified financial statements".

By far the biggest single risk that caused SOX to be enacted is that senior management's reward system provided massive incentives to distort short-term profits. Although there is no reliable statistical data in this area, a reasonable guess on the second biggest risk is that key accounting personnel lack the necessary skills to produce draft financial statements with zero material deficiencies without external assistance. A third major risk would be that the audit team assigned to complete the audit is not competent and/or objective. A more granular risk than #1 would relate to management initiated frauds related to stock options. A list of the top ten risks that have caused major errors in financial statements could be assembled fairly quickly from what has occurred in the past. Although a list of only the top ten risks wouldn't be enough for a comprehensive ICFR assessment exercise it would focus attention and resources on the really major risks at a fraction of the current costs.

SCALING THE AUDIT FOR SMALLER COMPANIES

PCAOB Draft Standard:

Page A1-8 states " the auditor should recognize that a smaller and less-complex company often achieves many of its control objectives through the daily interaction of senior management with company personnel rather than through formal policies and procedures."

IMA Analysis/Comment:

This may be a statement that recognizes the need for different approaches for SPCs but it doesn't really help an auditor to sign an opinion indicating that, in his or her professional opinion, ICFR control is effective. Our interpretation is that the auditor is staking his or her reputation and that of their firm that there is less than remote chance that management will produce draft financial statements with zero material defects. The reality is that smaller public companies often are less standardized in terms of business processes, contracting, and accounting policy and have a number of other attributes that can make assessing ICFR very difficult.

USING A TOP-DOWN APPROACH

PCAOB Draft Standard:

Page A1-11 states "A top-down approach begins at the financial statement level and company-level controls, and then works down to significant accounts and disclosures, relevant assertions and significant processes."

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

IMA Analysis/Comment: A true top-down approach should begin with formal identification and documentation of the major risks to the overarching objective of issuing materially reliable auditor certified financial statements.

IDENTIFYING COMPANY-LEVEL CONTROLS

PCAOB Draft Standard:

Page A1-11 states "The auditor must test those company-level controls that are important to the auditor's conclusion about whether the company has effective internal control over financial reporting."

IMA Analysis/Comment:

We applaud the PCAOB's efforts to improve the guidance in this area relative to AS2. The emphasis, however, appears to be on creating and testing a checklist of "company-level" controls. This may result in relatively junior audit firm staff equipped with standard questionnaires making inquiries about the company's strategic planning process, budget review process, code of conduct, audit committee performance, etc. Even a fully accredited CPA at the manager level is still relatively inexperienced in terms of assessing the effectiveness of a company's audit committee to detect management malfeasance, the impact the company's performance measurement/reward structure has on financial statement fraud vulnerability, and the company's risk assessment process. The current CPA examination body of knowledge has very little coverage of core risk management principles and global standards or focus on assessing ICFR using risk-based methods. The standard external audit does not generally include much involvement of the audit partner, the most experienced member of the audit team, in the actual field work. Without assessing likelihood and consequence of specific risks and then asking what company-level controls exist to mitigate it, evaluating company level controls lacks focus and can result in inaccurate conclusions on effectiveness.

IDENTIFYING SIGNIFICANT ACCOUNTS

PCAOB Draft Standard:

Page A1-14 states "the auditor should start by considering financial statement line items or captions. When identifying significant accounts, the auditor should evaluate both qualitative and quantitative **risk factors**."

IMA Analysis/Comment:

To be consistent with the intent of this statement, IMA believes that the auditor should identify and document the most significant risks to reliable disclosure (note: the level of risk significance is determined from specific combinations of likelihood and consequence) that threaten the reliability of accounts and notes to the financial statements.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Identifying "risk factors" is not the same as explicitly writing down significant risks and then considering the ability of one or more controls to mitigate the risk. For a risk-based approach to "resonate" with practitioners (SEC/PCAOB approaches), the use of standard risk management principles and generally accepted ISO risk terminology in the proposals is necessary.

Not employing "generally accepted risk principles" may be because so many accelerated filers have already completed their SOX ICFR assessments in the first 3 rounds without much emphasis on formal risk identification, documentation and measurement. There is no indication in SEC or PCAOB guidance that a company using a risk framework like AS/NZ 4360 or COSO ERM would be considered by the SEC or PCAOB to be using a "suitable" framework to assess the reliability of their ICFR system.

The risk identification and measurement step at the entity, subsidiary and account/note levels is a component that should be mandatory, not discretionary, in a true risk-based approach.

IDENTIFYING RELEVANT ASSERTIONS

PCAOB Draft Standard:

Page A1-15 states "For each significant account, the auditor should determine which of these financial statement assertions is a relevant assertion. – Existence or occurrence, Completeness, Valuation or allocation, Rights and obligations, Presentation and disclosure". It later states "The auditor should determine the likely sources of potential misstatements by asking himself or herself "what could go wrong"? within a given account."

IMA Analysis/Comment:

The word "assertion" is a traditional accounting term in use for many decades that has no meaning or relevance in the world of risk management. Even experienced auditors, when confronted with a note disclosure like the stock option disclosure, struggle trying to decide which "assertions" are the key ones. The emphasis on "assertion" identification results in the methodology used to assess ICFR being only relevant to accounting. Because the methodology can only be used to assess accounting reliability, companies cannot use the substantial investment they are making to implement SOX as a sound foundation for broader ERM efforts in other relevant areas that require formal assurance (e.g., safety, product quality, customer service, disaster preparedness, etc.).

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

IDENTIFYING MAJOR CLASSES OF TRANSACTIONS AND SIGNIFICANT PROCESSES

PCAOB Draft Standard:

Page A1-16 states "The controls over major classes of transactions exist within the company's significant processes. Accordingly the auditor should identify the significant processes affecting the major classes of transactions." It goes on to state that the auditor should "Identify the points within the process at which a misstatement – including a misstatement due to fraud – could arise that, individually or in combination with other misstatements, would be material; Identify the controls that management has implemented to address these potential misstatements….".

IMA Analysis/Comment:

At no point in the bullets that follow this statement does the draft standard explicitly state that the auditor should identify the controls in the processes that mitigate the risks they have identified. The use of the word risk in the guidance is missing.

PERFORMING WALKTHROUGHS

PCAOB Draft Standard:

Page A1-18 states "At the points at which important processing procedures occur, the auditor should question the company's personnel about their understanding of what is required by the company's prescribed procedures and controls. These probing questions are essential to the auditor's ability to gain a sufficient understanding of the process and be able to identify important points at which a necessary control is missing or not designed effectively."

IMA Analysis/Comment:

This is another illustration where the authors have not explicitly stated that during the walkthrough the auditor should have a list of the key risks clearly in mind that must be mitigated and focus on identifying where in the process or elsewhere those risks are mitigated, if at all. It isn't clear how an auditor can effectively focus only on key controls in the absence of specifically and visibly measuring risks and making the risk/control linkage.

SELECTING CONTROLS TO TEST

PCAOB Draft Standard:

Page A1-18 states "The auditor should test those controls that are important to the auditor's conclusion about whether the company's controls sufficiently address the addressed risk of misstatement to each relevant assertion."

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

IMA Analysis/Comment:

This is a good example of the impact on terminology by requiring the use of the term "assertion". Another way of stating this in a risk based approach is to simply state "The auditor should test the dominant controls that play an important role mitigating the significant risks to the account or note disclosure being evaluated".

PCAOB Draft Standard

Page A1-19 states "The auditor should focus on whether the selected controls, individually or in combination, sufficiently address the assessed risk of misstatement of a given relevant assertion rather than on how the control is labeled….".

The auditor should link the controls selected to test with the relevant assertions to which they relate."

IMA Analysis/Comment:

To properly assess the effectiveness of the controls in use using a risk management approach one must look at the "RESIDUAL RISK STATUS" that is being produced. A key element of this step is examining the current PERFORMANCE INDICATORS including detected account/note error rate. The standard makes no mention of residual risk identification or analysis as an explicit required step. These are central principles in all globally recognized risk management standards and the Basel II rules related to management of operational risk in banks around the world.

Attachment 1 to this comment letter provides IMA's risk-based framework, with more details contained in the 9/15/06 filing to the SEC.

TESTING DESIGN EFFECTIVENESS

PCAOB Draft Standard:

Page A1-20 states "The auditor should test the control design effectiveness of controls by determining whether the company's controls, if operating properly, satisfy the company's control objectives and can effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements."

IMA Analysis/Comment:

This guidance introduces the term "control objective" which sometimes means mitigating a relevant risk but sometimes means an objective to execute a control. The term "control objective" like the term "account assertion" is part of traditional accounting vernacular in use for many decades that has resulted in generally poor predictive results when assessing the true effectiveness of control design.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

This paragraph could read "The auditor should assess control design effectiveness by determining whether, in his or her opinion, the controls in place/use are likely to mitigate the risks that could result in a material error in the accounts to a level that precludes even a reasonable chance of a single material error".

RELATIONSHIP OF RISK TO THE EVIDENCE OBTAINED

PCAOB Draft Standard:

Page A1-21 states "For each control selected for testing, the auditor should assess the risk that the control might not be effective and, if not effective, the risk that a material weakness would result."

IMA Analysis/Comment:

In globally accepted risk management terms this statement would read something like: "The auditor must first determine whether the control(s) as described/understood is/are capable of mitigating the significant risks identified. Having completed that step, the auditor must test to verify that the control(s) is/are, in fact, being performed as described/understood. The auditor must then evaluate the residual risk status, or the degree the relevant risks are in fact being mitigated and form a conclusion whether the resulting residual risk position could allow a reasonable possibility of even a single undetected material account/note misstatement in draft financial statements."

STRONG INDICATORS OF A MATERIAL WEAKNESS

PCAOB Draft Standard:

Page A1-29/30 states: "The auditor should treat each of the following circumstances as a strong indicator that a material weakness in internal control over financial reporting exists – An ineffective control environment……
-Restatement of previously issued financial statements to reflect the correction of a misstatement…
- Identification of the auditor of a material misstatement in the financial statements in the current period in circumstances that indicate the misstatement would not have been detected by the company's internal control over financial reporting.
- Ineffective oversight of the company's external financial reporting and internal control over financial reporting by the company's audit committee.

IMA Analysis/Comment:

The IMA research study completed in 2006 indicates that the ability of auditors to assess and assign pass/fail grades to a company's control environment is not at a level capable of producing repeatable conclusions. The absence of agreed pass/fail criteria at a level of detail capable of producing repeatable conclusions is the key reason.

The large number of restatements and companies under investigation for stock option accounting errors supports this conclusion. Further research should be done to determine how many of these companies that have to restate their accounts had received a passing grade on their "control environment" from their external auditors under AS2 rules.

This is the section of the standard that indicates that if the auditor's examination of the accounts and note disclosures reveals even a single material error (NOTE: this could be defined as an error big enough the auditor will not sign-off on the accounts unless management makes the adjustment) they must, with few exceptions, indicate that the company has "ineffective control" in their SEC filing. This zero material defect standard is a level of quality that is more stringent than that applied in any other country in the world and is well beyond the level currently being delivered by literally thousands of U.S. listed non-accelerated filers.

The goal of zero material defects is laudable but may not be practical, especially in smaller public companies. The zero material defect rule in financial statement drafts and throughout the ICFR process is likely at the root of why smaller companies have sought and will continue to seek listings on exchanges in Canada, London and elsewhere. Both exchanges are considered to have generally good corporate governance requirements but neither has a standard that indicates a single material error in draft financial statements require management and/or auditors publicly indicate the company has an ineffective control system.

REPORTING ON INTERNAL CONTROL

PCAOB Draft Standard:

Page A1-36/37 calls for "The auditor's opinion on whether the company maintained, in all material respects, effective internal control over financial reporting as of the specified date, based on the control criteria …"

IMA Analysis/Comment:

This is at the heart of the debate whether Congress asked for an opinion on management's assessment or whether the auditor, personally, believes that ICFR is "effective". Reduced to the lowest common denominator, the auditor, under the current draft standards, is putting his or her name on the line, stating that they believe that the current controls will not allow even a single material error in the draft financial statements prepared by management. We believe that a significant percentage of U.S. non-accelerated companies that have not yet reported under Section 404 would fail this test. A large percentage of these companies are currently stating under section 302 rules that they have effective "disclosure controls". It is also virtually certain that if the zero material defect in the draft financial statements standard was applied rigorously in Canada, the UK and Europe, thousands of companies would be forced to publicly report they have ineffective internal control systems.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org

Whether a zero material defects in the financial statement drafts prepared by management is too stringent a quality standard should be carefully researched, including empirical evidence as to whether investors are better protected.

10 PARAGON DRIVE • MONTVALE, NJ 07645-1760 • TEL: 800-638-4427 • TEL: 201-573-9000 •
FAX: 201-474-1600 • www.imanet.org