



Response to

**Proposed Auditing Standard:
“AN AUDIT OF INTERNAL CONTROL OVER
FINANCIAL REPORTING PERFORMED IN
CONJUNCTION WITH AN AUDIT OF FINANCIAL
STATEMENTS”**

PCAOB Rulemaking Docket Matter No. 008

November 21, 2003

Prepared by:

Bruce W. McCuaig, B.Comm., CA•CIA, CCSA

Tim J. Leech, FCA•CIA, CCSA, CFE, MBA

CARD[®]decisions Inc.

2655 North Sheridan Way, Suite 150

Mississauga, ON, Canada, L5K 2P8

Tel: (905) 823 5518

Fax: (905) 823 5657

www.carddecisions.com

**CARD[®]decisions Response to
Proposed Auditing Standard:**

**“AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL
REPORTING PERFORMED IN CONJUNCTION WITH AN
AUDIT OF FINANCIAL STATEMENTS**

TABLE OF CONTENTS

| | Page # |
|--|---------------|
| Executive Summary | 1 |
| CARD[®]decisions Specific Responses | 7 |
| (#1-3) Questions regarding an integrated audit of the financial statements and internal control over financial reporting | 7 |
| (#4) Question regarding the costs and benefits of internal control | 10 |
| (#5) Question regarding the audit of internal control over financial reporting | 11 |
| (#6 – 8) Questions regarding evaluation of management's assessment | 13 |
| (#9 – 10) Questions regarding obtaining an understanding of internal control over financial reporting | 16 |
| (#11) Question regarding testing operating effectiveness | 18 |
| (#12 – 16) Questions regarding using the work of management and others | 18 |
| (#17 – 24) Questions regarding evaluating results | 22 |
| (#25 – 27) Questions regarding forming an opinion and reporting | 25 |
| (#28 – 29) Questions regarding auditor independence | 26 |
| (#30 – 31) Questions regarding auditor's responsibilities with regard to management's certifications | 27 |
| Professional Profiles | 28 |

EXECUTIVE SUMMARY

Will the draft standards improve the quality and quantity of information on internal control over financial reporting?

Our view is no, they will not. We believe Congress intended to reinforce management's accountability for reliable financial reporting by requiring auditors evaluate and form an opinion on management's assertions on internal control effectiveness. These standards are primarily for auditors to form a direct subjective opinion on internal control effectiveness through traditional audit approaches. These approaches have been in use for decades and have often proven to be ineffective.

The standards require significant revisions to focus the attention of external auditors on opining on the reliability of management's assertions on control and to guide the auditor in forming an opinion directly on the quality of those assertions.

Will the draft standards improve the capability and motivation of managers and work groups to provide more reliable assertions on internal control effectiveness and to be accountable for those assertions?

Our view is no, they will not. There is little guidance for auditors, managers, work groups Boards or any other stakeholder on the various approaches, methodologies, tools and technologies available for assessing, designing, documenting and reporting on internal control effectiveness.

There is little incentive for managers and work groups to fully and candidly divulge disclosure risks, particularly those classified as "material weaknesses".

The standards as drafted are dominated by a discussion of controls (1309 references) in the absence of serious attention to and analysis of disclosure risks (76 references). Although the proposals will generate substantial revenue for the external auditing profession and add a major ongoing assurance burden in companies, we believe they will do little to cost effectively solve the real problems.

The standards require significant revision to recognize and discuss the approaches, methodologies and tools used by assurance professions, particularly the use of criteria based approaches to forming an opinion on the quality of and reliability of management assessments.

Will the draft standards help drive down or even justify the cost of control over financial reporting?

Our view is no, they will not. They simply justify more auditing and more controls. They provide little guidance or useful definition as to what constitutes effective control and material/significant deficiencies. We believe the standards as drafted will result in a large increase in formal assurance costs with only limited positive impact.

The standards should be significantly revised to recognize more powerful and objective approaches to documenting, assessing, designing and reporting on controls and control effectiveness and to assessing the cost effectiveness of controls over financial reporting.

GENERAL COMMENTS

General comments on the Proposed Standards are set out here.

1. Will these proposed standards increase the quality and quantity of information on risks and controls related to financial disclosure?

The standards as drafted will not produce more and better information on risk and control over financial reporting.

For the most part, stakeholders will be given Pass/Fail assessments of internal control effectiveness over financial reporting developed by external auditors, supplemented by explanations of significant deficiencies or material weaknesses. The basic design of the internal control framework, its strengths and accepted deficiencies will not be reported to stakeholders. There is no framework for doing so proposed in these standards.

We see the continuation in this standard of subjective belief-based, not fact-based, auditor-driven opinions on what constitutes effective control.

We see little guidance to help auditors assess and report on the reliability of management's assertions on internal control effectiveness.

The standards as drafted struggle with concepts of "deficiencies, significant deficiencies and material weaknesses" that are for all practical purposes, indefinable and subjective to a degree that makes external disclosure of these subjective views dangerous.

Other assurance professions, most notably quality, environmental and safety professionals have developed very effective tools, methods and criteria for evaluating and reporting on risk and control in their fields. They have created meaningful analytical tools useful for identifying root cause problems and providing practical, rather than dogmatic solutions.

What is needed?

What is needed is a paradigm shift.

Stakeholders need to be able to come to their own conclusion on the role of internal control effectiveness in investment decisions and to be able to make risk acceptance decisions based on the stated level of internal control effectiveness in a corporation. A framework for gathering and reporting this information is required. Pass/Fail assessment do little to meet these needs.

Stakeholders need to be able to compare changes in a company's internal control structure over time and to compare one company to another, just as they now compare financial statements.

The information in disclosures on internal control effectiveness likely to result from these proposed standards will not support such an analysis.

It would be unthinkable to replace published financial statements with an auditor's subjective opinion on a company's financial health.

It is not sufficient to provide an opinion on internal control effectiveness without a positive framework to support such an opinion.

What is needed is a criteria-based approach to evaluating internal control over financial reporting.

Bond rating agencies rate corporate debt against defined criteria and publish credit ratings that have real financial consequences for creditors and that are relied upon by investors.

In the quality movement, the Baldrige model is an example of a system that measures a company's quality framework against defined, weighted, published criteria. ISO standards provide another example. Management makes assertions as to the criteria in place and auditors evaluate the reliability of those assertions.

The Basel Capital Accord on bank safety (Basel II) provides another powerful framework for assessing governance and the management of risk and control.

Principles from all of these frameworks could be adapted to reporting on internal control effectiveness over financial reporting.

The auditing profession, internal and external, has consistently failed to predict governance failures in the past. There is no reason to believe these proposed standards will make a difference, other than reducing returns to shareholders and retarding economic growth.

We believe the auditing profession can best add value by providing a framework for disclosing information on risk and control status such that stakeholders can make their own informed investment decisions.

2. Do these proposed standards improve the capability of managers, work groups and others to make reliable financial disclosures and to make reliable assertions on the effectiveness and status of risk and control over financial reporting?

Our conclusion is no, they do not.

The proposed standards do recognize the need to address the capability of auditors in the area of control assessment. They do not address the capability required by managers and work groups to make and support reliable assertions on internal control effectiveness over financial reporting. They do not define a common body of knowledge, tools, methodologies, approaches or technologies for assessing and reporting on internal control effectiveness over financial reporting. COSO 2003 can help in that regard. COSO 1992, although a big advancement in 1992, is not up to the task.

In order to conclude that the capability of managers and work groups to provide more reliable assertions on the status of risk and control over financial reporting is increased, much more is required to provide Boards, managers, work groups and auditors with skills training, rigorous, reliable methodologies and useful tools for describing, assessing, designing and reporting on internal control effectiveness and standards for assessing the reliability of those assertions.

For the most part, the proposed standards speak a language that is outmoded and invalid. The draft standard provides little in the way of analytical tools and guidance to managers and work groups. They appear to represent control assessment beliefs that have been in use for decades. The same decades that numerous corporate governance failures have occurred.

What is needed?

We believe that the required body of knowledge exists and the skills, methodologies and tools to increase the capability of all those involved in the financial reporting process are available. In our response to Question 5 we have provided some specific examples.

3. Will these proposed standards motivate managers and work groups to provide better and more reliable information and disclosures on risk and control related to financial reporting?

Our conclusion is no, they will not.

Managers and work groups who report “deficiencies” will effectively and immediately be penalized with adverse opinions by their auditors, more burdensome internal controls, negative market reactions and higher external audit fees. Yet we know “deficiencies” in internal control over financial reporting as defined in the proposed standards have existed for decades in hundreds even thousands of successful public companies.

As written, the proposed standards require auditors to recognize the quality of work done by managers and work groups in supporting their assertions on internal control effectiveness, but the proposed standards require substantial direct verification of internal control by auditors rather than examining and focusing on the reliability of management’s representations on control and risk status.

Unless the burden of accountability for making reliable assertions on internal control over financial reporting is clearly and exclusively assigned to managers and work groups, and they are evaluated specifically on the quality and reliability of their representations, their motivation to do so competently and reliably will be weak. Auditors will do it for them. Why should they do it themselves?

What is required?

We believe the standards should be revised to encourage a risk based approach to control design, to encourage management's candid disclosure of significant residual risks and where unacceptably high residual risks exist, to provide management with recourse to substantiate external disclosure with supplemental substantive testing and confirmation.

Standards that promote direct examination of internal control effectiveness by auditors will inevitably shift accountability away from management and with it any motivation for providing reliable representations.

Stakeholders deserve to know the quality of management's representations on the effectiveness of the external disclosure risk management systems those managers design and maintain.

4. Will these proposed standards allow a reduction in the cost and burden of implementing effective control over financial reporting?

We believe the standards as proposed will significantly increase the cost of control and the cost of non-value adding assurance. We are concerned that the increase in control will not be justified and will not result in more effective internal control over financial reporting and will not produce more reliable financial disclosures.

We believe the standards as proposed provide the auditor with justification to do more auditing. They do not add value for stakeholders of the financial reporting process.

The proposed standards use the word control(s) a total of 1309 times and the word risk(s) 76 times. All of the major advances in this field over the past decade center on identifying and measuring risks first, and only when that step has been done, and done well, examining mitigators/controls.

While word counts in the proposed standards may be only a crude measure of their emphasis and balance, we do not believe that the increased emphasis on examining controls in a vacuum from risks is appropriate.

We believe the notion of judging the design and operating effectiveness of controls as proposed in these standards, in isolation from risk or from a competent assessment of cost/benefit is fundamentally flawed.

What is needed?

The standards should be revised to give equal weight to identifying risks, examining controls and evaluating the current acceptability of the current residual risk status.

We believe the standards should adopt the concept of a portfolio of controls and an assessment of residual risk over each major disclosure line item, note and supplemental disclosure.

We believe an explicit assessment of residual risk (using an acceptable risk model and a criteria based control model) for each disclosure line item or note is intellectually more reliable and much more useful than an auditor's subjective opinion on control effectiveness.

We believe that by providing support for assertions on control effectiveness over external financial reporting management should also demonstrate they have driven the cost of control to the lowest level possible that produces an acceptable level of residual risk. To not focus on both elements in concert does a disservice to investors and to society in general.

CARD[®] decisions' Response to PCAOB

Questions regarding an integrated audit of the financial statements and internal control over financial reporting:

1. Is it appropriate to refer to the auditor's attestation of management's assessment of the effectiveness of internal control over financial reporting as the audit of internal control over financial reporting?

Response: No. Management must be required to make and substantiate assertions on internal control effectiveness over financial reporting.

The auditor's opinion must be focused on the reliability of management's assessment of internal control over financial reporting.

An auditor's attestation of management's assessment of internal control and an auditor's direct opinion on internal control effectiveness are significantly different and are arrived at using different audit procedures.

Few, if any, of the recent corporate governance failures were predicted by either internal or external auditors from their direct opinions on internal control effectiveness. This is true in spite of companies spending large sums on internal and external auditors.

Requiring management to make and support assertions on internal control effectiveness, and requiring auditors to form an opinion on the quality and reliability of those assertions will dramatically improve the quality of financial reporting.

The auditing profession has not demonstrated that it is capable of forming consistently reliable opinions on internal control effectiveness. There is nothing in these draft standards to address that severe and historic deficiency since it encourages the use of methods that have been in use for over 25 years and a control model developed 12 years ago.

To suggest that auditors must prove the reliability of management's assertions primarily by performing their own direct audit of internal control effectiveness suggests that the profession does not know how to distinguish a reliable set of management assertions on internal control effectiveness from an unreliable set of assertions on internal control effectiveness.

These standards as drafted recognize the need for the auditor to review management's assessment of internal control over financial reporting, but they stop well short of what is required to form an opinion on the quality and reliability of management's assessment. Instead, they are primarily draft standards guiding the auditor in providing their own separate and direct opinion on internal control. Unlike an auditor's opinion on management's assertions over its financial statements,

CARD[®] *decisions*' Response to PCAOB

little guidance is provided for managers to prepare and support a reliable assertion on internal control effectiveness over financial reporting.

There is no basic principal of organizing information on internal control assertions analogous to the way financial statements organize and present financial information.

There are no generally accepted and useful criteria of risk and control analogous to GAAP, and there are no adequate standards to guide auditors in forming an opinion on those management's assertions on internal control.

The standards, guidance and criteria for management to make assertions and auditors to form opinions on assertions on internal control over financial reporting are a huge missing link in the financial reporting process and one the Board is in an historic position to remedy. COSO ERM 2003 provides an initial, partially useful framework. COSO 1992 is not sufficient.

In order for an auditor to provide an opinion on management's assertions, new standards are required to provide a basis for an auditor to provide such an opinion. Such standards would require development of criteria of risk and control against which management's assessment could be measured and would require the recognition of methodologies and tools appropriate for management and work groups to use. Such standards would also specify the knowledge and skills required by management in order to prepare an assertion on internal control effectiveness.

Precedent exists for the development of such criteria and standards. The Baldrige quality model is an example of weighted criteria against which an organization's ability to produce quality products and services can be judged. Similar models and criteria exist to judge safety.

The Baldrige criteria and effective safety frameworks are based on the premise that quality and safety cannot be "inspected" into an organization.

The Basel Capital Accord on bank safety (Basel II) provides a powerful framework for assessing governance and the management of risk and control.

The history of the auditing profession would suggest that reliable financial reporting will not be "audited" into organizations.

A new paradigm is required by the auditing profession.

The PCAOB should significantly revise these draft standards to provide guidance for managers and work groups to make reliable assertions on internal control effectiveness and for auditors to form an opinion on the reliability of those assertions.

CARD[®] decisions' Response to PCAOB

2. Should the auditor be prohibited from performing an audit of internal control over financial reporting without also performing an audit of the financial statements?

Response: No.

The question should be reversed.

“Should the auditor be prohibited from performing an audit of the financial statements without first forming a satisfactory opinion on the reliability of management’s assertions on control effectiveness over financial reporting?”

The answer to the question framed this way is yes. Reliable management assertions on internal control effectiveness should be a prerequisite for an auditor to proceed with the audit of financial statements.

An opinion that management’s assertions are not reliable should be considered a material weakness. An audit of the financial statements should not be undertaken until management provides reliable assertions on the status of internal control over financial reporting.

Assessing the reliability of management’s assertions on internal control effectiveness should be the subject of a separate standard, however forming an opinion on the reliability of those assertions will likely involve some reperformance of procedures or substantiation of financial statement amounts.

If the auditor finds management’s assertions on control effectiveness reliable and, subsequently, during the audit of the financial statements, finds information to contradict the assertions being relied upon, a material weakness should be declared.

3. Rather than requiring the auditor to also complete an audit of the financial statements, would an appropriate alternative be to require the auditor to perform work with regard to the financial statements comparable to that required to complete the financial statement audit?

Response: No.

Evaluating and testing the basis for and reliability of management’s assessment of internal control over financial reporting is significantly different than an audit of the financial statements.

It says little for the concept of internal control over financial reporting and management’s assertions if professional auditors cannot directly examine internal control and the quality of management’s assertions without performing an audit of the financial statements. This does not mean that substantive testing will not be required.

CARD[®] decisions' Response to PCAOB

If the only evidence of the reliability of internal control over financial reporting or management's assertions thereon lies in the accuracy of the financial statements, the notion of any evaluation of internal control should be abandoned.

Question regarding the costs and benefits of internal control:

4. Does the Board's proposed standard give appropriate consideration to how internal control is implemented in, and how the audit of internal control over financial reporting should be conducted at, small and medium-sized issuers?

Response: Yes. Management may choose to develop its assertions on internal control effectiveness over financial reporting in a variety of ways and to rely in its assertions on various types and levels of internal control to achieve its financial reporting objectives.

The proposed standards recognize the concept that effective control can be achieved in a variety of ways.

However far better criteria are required to define more definitively what is meant by effective internal control over financial reporting and the notion of its equifinality.

Pass/Fail approaches to evaluate internal control effectiveness are inappropriate and do not provide the information required by stakeholders. Imagine if credit ratings were reduced to Pass/Fail judgments.

COSO 2003 provides a starting point for identifying and categorizing criteria of control, but both the original and proposed revision to COSO are far too broad to support detailed analysis, design or assessment of the status of risk and control systems.

A strong argument can be made that COSO 1992 does not meet the Board's criteria for a suitable framework for management's assessment of internal control. Although a major contribution in 1992, it has not progressed and, unlike Baldrige or the ISO standards, does not have an improvement framework.

A strong argument in favor of the proposed 2003 COSO is its inclusion of an enterprise risk framework and a process. This is essential.

Modern assurance practitioners must insist on a rigorous risk assessment as a first step in the design, evaluation or testing of controls.

In order for management to make reliable assertions on control effectiveness over financial reporting, they must develop or be provided with tools they can use to design, evaluate and report on risk and control and these tools must be practical and understandable.

CARD[®] decisions' Response to PCAOB

It will not be possible to ask management to make reliable assertions on internal control effectiveness with the tools the profession has provided them with to date. COSO speaks an auditor's language, not the language of a manager or work group.

Question regarding the audit of internal control over financial reporting:

5. Should the Board, generally or in this proposed standard, specify the level of competence and training of the audit personnel that is necessary to perform specified auditing procedures effectively? For example, it would be inappropriate for a new, inexperienced auditor to have primary responsibility for conducting interviews of a company's senior management about possible fraud.

Response: Yes.

Guidance is essential in this area. The knowledge and skill required to competently evaluate control has increased enormously. The profession has a widespread reputation for promoting low level control practices and relying on micro control activities whose worth is dubious in the absence of any evaluation of the underlying disclosure risk.

It is worth noting that these draft standards proposed by the Board, contain over 1300 references to control(s) and only 76 references to risk(s), a strong indication of their focus.

Professional audit practices, tools, approaches or skills have not fundamentally changed in recent years in spite of evidence that old ways of auditing have often failed.

Substantial changes must be made in the body of knowledge, the skills, practices and technology used by the profession.

Furthermore, it is an appropriate role of the auditing profession, if not the Board, to suggest the knowledge, methodologies, standards, tools and skills required by management to make reliable assertions on control effectiveness over financial reporting.

Ideally, the guidance in these draft standards should be understandable and useful to managers in making their assertions and not just used by auditors in forming opinions on management's assertions.

The very definition of internal control over financial reporting could be dramatically simplified to refer to anything management or work groups do to manage risks and achieve reliable external financial reporting.

The auditing profession and management has consistently underrated the knowledge

CARD[®] decisions' Response to PCAOB

and skills required to design, implement, sustain and evaluate cost effective systems of internal control.

Examples of some of the knowledge required of modern auditors are:

- COSO 2003 or alternative approach to risk and control design and assessment such as the ANZ Risk Management Standards.
- Defining and prioritizing risks and financial disclosure objectives.
- Using generally accepted risk source models and other techniques to identify categorize and evaluate risks/threats to financial disclosure for the entire organization, sub-units, specific accounts and note disclosures and to create specific disclosure objectives and disclosure risk profiles/risk maps.
- Critically evaluating and using control models such as COSO and CoCo to identify, evaluate and optimize the cost of control portfolios.
- Developing reliable descriptions of residual risk status including concerns, indicator data, impact information, impediments with respect to internal controls over financial disclosure.
- The five major approaches to direct report audits and management self-assessments and business reasons for adopting self-assessment approaches to risk and control management. (Note that these Draft standards recognize only one of these five approaches).
- Barriers and implementation strategies for self-assessment approaches as a means of obtaining management assertions on risk and control and related risk acceptance decisions.
- The evolution of Generally Accepted Control Criteria ("GACC") including all major control and quality models.
- The evolution of Generally Accepted Risk Criteria ("GARC") including the leading risk standards and frameworks from around the world.
- Integrating insurance and risk transfer decisions with risk and control design analysis and decision-making.
- Linkages between Basel Committee requirements for financial institutions in the area of risk and control and the linkages between the 5 stages of enterprise risk management described in *Operational Risk: The Next Frontier* study published by the RMS, ISDA and British Bankers Association and other major approaches such as COSO 2003..
- The business case and benefits for enterprise risk management system as a means of driving, integrating and sustaining ongoing assessments and evaluations of internal control over financial reporting.
- Strategies to integrate performance management, risk and control management,

CARD[®] decisions' Response to PCAOB

assurance management and knowledge management with financial reporting.

- Completing quality assurance reviews (audits) of risk and control analysis completed by management and work units to evaluate the reliability of management's assertions.
- Basic principles used to develop estimates of the cost of control and the cost of assurance

Questions regarding evaluation of management's assessment:

6. Is the scope of the audit appropriate in that it requires the auditor to both evaluate management's assessment and obtain, directly, evidence about whether internal control over financial reporting is effective?

Response: No.

An auditor's opinion focused on the reliability of management's assertions on internal control effectiveness over financial reporting is required.

Such an opinion would require an evaluation of the scope, processes, tools, methodologies, participants, and quality procedures in place and used by management in preparing and supporting their assertions on internal control effectiveness.

Such an opinion would also require some direct examination of evidence of internal control, but the opinion itself and the focus of the audit evidence would be on the reliability of management's assertions and not on opinion on internal control effectiveness.

Management must be fully responsible for its opinion on internal control effectiveness and status.

These draft standards do not provide sufficient guidance to allow an auditor to express such an opinion.

If the existence of effective systems of internal control and the reliability of management's assertions over internal control effectiveness cannot be directly examined and opined on, as opposed to an examination of the results of effective internal control, then the profession should remove any discussion of internal control from its standards and focus entirely on substantive verification of account balances and reliability of note disclosures.

An auditor's direct evaluation of internal control over financial reporting has been historically unreliable, will be not be improved by these draft standards, and is not in any way a substitute for an opinion on management's assertions on control effectiveness over financial reporting.

CARD[®] decisions' Response to PCAOB

7. Is it appropriate that the Board has provided criteria that auditors should use to evaluate the adequacy of management's documentation?

Response: No.

Criteria to evaluate the adequacy of management's documentation is secondary.

Criteria are needed to evaluate the reliability of management's assertions on internal control over financial reporting.

Specifically, criteria are needed to evaluate the scope, processes, tools, methodology, participants, quality assurance mechanisms management and technology, if any; management uses to make its assertions on internal control effectiveness.

Standards governing documentation may be a subset of the broader criteria. But the extent and quality of the documentation is secondary to the content and procedures the auditor must follow.

Specifically, there is no provision in the draft standards relating to the auditor's evaluation of management's assessments of risk to determine what could prevent adequate disclosure for financial statement line items, note disclosure or other matters. For example, what constitutes a sufficient analysis of risks to a reliable external disclosure as a basis for identifying critical controls that should be tested is not discussed.

There is no reference to the use of risk models in assessing risk. While the use of COSO 2003 is encouraged, its flaws when used for more than macro level risk and control analysis and design at a specific disclosure process level are not recognized in these draft standards.

Arguably the original 1992 COSO framework does not meet the requirements for a framework suggested by these draft standards. The 2003 revisions are preferable in that they still require some risk assessment but they require improvement to be useful to management.

Only one approach, the process based assessment approach, is suggested in this standard as a methodology for assessing controls related to financial disclosure. At least four other assessment approaches are in general use individually or in combination.

There is little reference to the use of control and risk self-assessment approaches or guidance on how or where such approaches may be appropriate to evaluate risk and control in spite of the use of self assessment by many assurance professionals and many companies.

CARD[®] decisions' Response to PCAOB

Without a rigorous risk assessment, key controls will not be identified, assessed or documented by management or properly considered by auditors. Nor is it likely that management will find the control evaluation process credible and valuable.

These draft standards are overwhelmingly focused on imposing controls that the auditor subjectively believes may be effective. A word count reveals that the word control(s) appears over 1300 times in the draft standards while the word risk(s) appears only 76 times.

The draft standards do not provide guidance on what constitutes adequate risk assessment and only limited guidance on tools, methodologies and approaches to assess, design and report on control effectiveness.

An opinion on management's assertion on internal control effectiveness is not possible without reviewing the quality of managements risk assessment over disclosure.

8. Is it appropriate to state that inadequate documentation is an internal control deficiency, the severity of which the auditor should evaluate? Or should inadequate documentation automatically rise to the level of significant deficiency or material weakness in internal control?

Response: Yes.

The questions posed in #8 are too narrow. The draft standards should deal with far more than documentation. The draft standards should deal with the content as well as the amount and quality of the documentation. Ideally the draft standards would also recognize, if not prescribe, the appropriate use of technology for documentation of risks, controls and residual risk status.

Management can and must be responsible for defending its assertions on control effectiveness over financial reporting. In addition to documentation, the auditor should examine the scope, processes, methodology, approach, participants, and tools, including technology, used by management in documenting risk, control and residual risk acceptance decisions.

The reliability of management's assertions on internal control effectiveness can be called into question if any of these factors are flawed.

CARD[®] decisions' Response to PCAOB

Questions regarding obtaining an understanding of internal control over financial reporting:

9. Are the objectives to be achieved by performing walkthroughs sufficient to require the performance of walkthroughs?

Response: Yes.

Walkthroughs are a minor part of the auditor's examination and insufficient to form an opinion either on management's assertions or on internal control itself.

Another more relevant way of asking the question is "Are the criteria sufficient to evaluate management's assertions on internal control effectiveness or to directly verify internal control effectiveness discernable to an auditor performing a walkthrough of the company's significant financial processes?"

The answer to that question is no.

Walkthroughs in the context of these draft standards take place at the transaction or system level. They may be an appropriate measure where the auditor requires evidence that processes are functioning as described by management. But they are not worthy of the attention they receive or the reliance placed on them in these draft standards.

They are indicative however of the relatively narrow view of internal control implied by the draft standards.

Many modern criteria based control and quality frameworks weigh leadership, capability, measurement and commitment far more heavily than the control activities susceptible to walkthroughs. In fact, some virtually ignore micro level control activities on the theory that if the broader elements are in place, control activities will follow.

Generally, breakdowns in control activities that would be seen in walkthroughs should be seen as symptoms of fundamental control issues and not as problems in and of themselves (e.g. employee failure to comply with a policy may be a symptom of poor training or a failure of management to make objectives and priorities clear).

What role did failures of transaction based processes play in the fraudulent and inaccurate financial reporting of the last decade? Little or none in many instances.

It is unlikely that walkthroughs would have detected the root causes of fraudulent financial reporting and inaccurate financial disclosure that these draft standards attempt to address.

The root causes of fraudulent financial reporting do not lie at the process or transaction

CARD[®] decisions' Response to PCAOB

level of the organization.

When criteria are developed for the evaluation of internal control over financial reporting, the usefulness of walkthroughs as an evaluative procedure can be assessed.

The corporate financial reporting failures that led to the formation of the PCAOB will not be found by walkthroughs.

Walkthroughs might reveal individual process failures or inefficiencies but they will not look on the right level, on the right things, on the right behaviors or on the right people to be of significant use to achieve the goal of these draft standards.

The extent of their use should be a matter for practitioner discretion and not a matter for these draft standards.

Effective Internal control over financial reporting lies in the behavior of the organization's leaders and its employees. The quality of the organization's leadership and its influence on the behavior of the organization must be considered.

Unreliable financial reporting is essentially a quality problem. The quality movement has determined that the drivers of quality in manufacturing, like the drivers of quality in financial reporting, begin far from the factory floor.

10. Is it appropriate to require that the walkthrough be performed by the auditor himself or herself, rather than allowing the auditor to use walkthrough procedures performed by management, internal auditors, or others?

Response: No.

It is appropriate for the auditor to query management's processes for evaluating and reporting on the effectiveness of internal control over financial reporting.

It is appropriate for the auditor to ask management how they ensure that controls are operating as described.

If management does not perform a walkthrough of significant processes, or demonstrate reliable knowledge of the controls in use, a deficiency should be noted and the reliability of their assertions on internal control effectiveness adjusted downward by the auditor.

Where management is relying on controls susceptible to verification by walkthrough, it is reasonable for the auditor to ask for evidence of the walkthrough.

CARD[®] decisions' Response to PCAOB

Question regarding testing operating effectiveness:

11. Is it appropriate to require the auditor to obtain evidence of the effectiveness of controls for all relevant assertions for all significant accounts and disclosures every year or may the auditor use some of the audit evidence obtained in previous years to support his or her current opinion on management's assessment?

Response: No.

It is management's job to obtain evidence of the effectiveness of controls annually, management's job to determine the most relevant assertions annually and management's job to demonstrate annually to the auditor that they have done so and done so reliably.

It is the auditor's job to form an opinion on the reliability of management's assertions.

In the course of forming an opinion on management's assertions it will be appropriate to review some of the evidence provided by management to support their assertion.

Accordingly, for the most part, the evidence the auditor will be obtaining to support an opinion on management's assertions will be based on the evidence management provides. Such evidence will consist of the scope, processes, tools, level and quality of employee involvement, approach used and technology employed as well as information on risks, controls and residual risk status with respect to achieving the objectives of reliable financial reporting.

In particular, in evaluating management's assertions on control effectiveness over financial reporting, the auditor should pay particular attention to the risk assessment process undertaken by management to identify and evaluate the risks to accurate financial reporting.

Questions regarding using the work of management and others:

12. To what extent should the auditor be permitted or required to use the work of management and others?

Response: The work performed by management and others in forming an opinion on internal control effectiveness should be the primary source of audit evidence.

The auditor should be required to specifically evaluate the quality and reliability of work provided by management and others and to assess and report its reliability. In particular this includes management's representations on the controls in use and on residual risk status.

CARD[®] decisions' Response to PCAOB

If the auditor does not find the work performed by management or others to be complete, accurate or reliable, the auditor should provide an opinion to that effect.

Assessing the reliability of work performed by management and others may include reperformance of portions of that work.

However, only if and when the auditor cannot rely on the assessment work of management and others should it be disregarded.

Where the work performed by management and others to form an opinion on internal control effectiveness is insufficient and unreliable, the deficiency should be remedied before the auditor proceeds to express an opinion on the financial statements.

These draft standards should provide specific guidance on how to form an opinion on the reliability of assessment work performed by management and others.

13. Are the three categories of controls and the extent to which the auditor may rely on the work of others appropriately defined?

Response: No.

The three categories of controls, specifically those that are part of the control environment, controls over the period end financial reporting process and controls that have a pervasive effect on the financial statements, if they are truly important, are exactly the areas where management must make and support its strongest assertions.

These three areas are those in which the auditor must provide the highest level of assurance over management's assertions.

If an external auditor cannot rely on management's assertions in these areas, they should report a material weakness and not proceed further until the inaccurate or even fraudulent assertions are remedied.

This places a significant and completely appropriate burden on management to honestly and competently describe, document and support their assertions in these areas. It places a significant and completely appropriate burden on the Board and the profession to provide the necessary standards and criteria to guide management in preparing and documenting their control effectiveness assertions.

The auditing profession has not demonstrated to date that it is capable of directly and consistently providing reliable opinions on internal control effectiveness in these areas. Management letters on control produced by external auditors have been criticized by our clients all over the world.

These are precisely the areas where investors and all other stakeholders must find

CARD[®] decisions' Response to PCAOB

management's assertions reliable and where an auditor's opinion on the reliability of those assertions will have most value.

This is the area where the PCAOB should be focusing its standard setting activities.

Forming an opinion on management's assertions will require verification by the auditor and the extent and nature of the verification will be based to some degree on professional judgment and will involve some degree of reperformance to test the reliability of management representations.

But if management cannot or does not provide reliable representation on control effectiveness, all stakeholders who rely on an auditor's opinion should be told.

14. Does the proposed standard give appropriate recognition to the work of internal auditors? If not, does the proposed standard place too much emphasis and preference on the work of internal auditors or not enough?

Response: No.

These draft standards do not appropriately recognize the role played today by internal auditors, the role they could play in the future and the value of the work they perform.

Internal auditors are an important part of the internal control framework and the work they do must be evaluated as part of the audit of management's assertions on internal control over financial reporting.

A new and very appropriate role of internal auditors is to evaluate the organizations risk and control management's processes. This is one of the new Internal Audit Standards issued by the Institute of Internal Auditors. If internal auditors are professionally and technically competent and provide reliable information on the state of internal control and the reliability of management representation on risk and internal control management, it should be relied upon to a significant degree.

If the work of internal auditors is found to be unreliable, the external auditor should report a major deficiency in internal control that is, with certainty, a material weakness.

Failing to assess the quality and competence of the work performed by internal auditors as a basis for relying on such work is a significant omission in these draft standards.

Internal auditors must be held fully accountable for the quality of their work. That includes work assessing control directly and work reporting the reliability of management self-assessments.

CARD[®] decisions' Response to PCAOB

15. Is the flexibility in determining the extent of reperformance of the work of others appropriate, or should the auditor be specifically required to reperform a certain level of work (for example, reperform tests of all significant accounts or reperform every test performed by others that the auditor intends to use)?

Response: No.

Flexibility in determining the extent of reperformance of the work of others is appropriate.

Reperformance may be efficient, but reperformance is not a substitute for forming an opinion on the reliability of management's assertions on internal control effectiveness.

Reperformance should primarily be considered as a means of obtaining assurance where the highest level of assurance is required. The extent of its use should be at the discretion of the auditor and not mandatory.

16. Is the requirement for the auditor to obtain the principle evidence, on an overall basis, through his or her own work the appropriate benchmark for the amount of work that is required to be performed by the auditor?

Response: No.

Management is responsible for providing the principal evidence to support internal control effectiveness representations.

The auditor is responsible for obtaining evidence that management's assertions are reliable. Evidence for this opinion will primarily lie in an examination of the scope, tools, procedures, methodologies, approaches, participants and technology employed by management in arriving at the assertion.

The amount of work to be performed by the auditor should be directly related to the quality of management's assertions on internal control effectiveness.

Standards to guide the auditor in the evaluation of management's assertions are required and those standards should address the amount of principal evidence on internal control effectiveness to be obtained by the auditor.

CARD[®] decisions' Response to PCAOB

Questions regarding evaluating results:

17. Will the definitions in the proposed standard of significant deficiency and material weakness provide for increased consistency in the evaluation of deficiencies? How can the definitions be improved?

Response: No.

It is safe to assume that every company required to report under Sections 302 and 404 will have, at any given time, a number of deficiencies, many of them significant.

It is also safe to assume that every public company will, over time, have one or more material weaknesses.

Candid disclosure and correction of significant deficiencies and material weaknesses will be discouraged by these draft standards.

The quality of a company's system of internal control over financial reporting and management's assertions should be rated and disclosed with reference to criteria.

Investors, regulators and other stakeholders may make their own judgments and act accordingly.

Similarly, public companies will occasionally experience financial losses or write-offs.

Denying an opinion on financial statements because of a financial loss or write-off would not be acceptable.

Investors, employees and other stakeholders may come to their own conclusion on stakeholder risk when given reliable information on the external disclosure processes.

The Baldrige quality model provides for scoring an organizations quality framework against a set of weighted, predefined criteria. The criteria are regularly updated and improved.

Bond rating agencies similarly score and publish corporate credit ratings based on established criteria related to credit worthiness.

Some rating organizations are assigning and publishing corporate governance ratings for public companies based on defined and disclosed assessment criteria.

The Board and the auditing profession have the opportunity to develop a similar method for assigning a score or rating on internal control effectiveness.

Such a system, to be credible and rigorous, would require input from the profession and

CARD[®] decisions' Response to PCAOB

from companies. It would allow investors and others to compare companies over time and across industries.

Defined criteria would be updated regularly. It would make the evaluation of internal control effectiveness transparent to management, employees, other stakeholders, auditors and regulators.

18. Do the examples in Appendix D of how to apply these definitions in various scenarios provide helpful guidance? Are there other specific examples that commenters could suggest that would provide further interpretive help?

Response: No.

Examples must focus on situations where management's assertions are determined to be unreliable.

Examples should also include situations where management has disclosed significant deficiencies or material weaknesses and proposed remedies or substituted other procedures to support the reliability of external disclosures.

For years, external auditors have chosen, in their audit of financial statements to perform substitute substantive testing rather than rely on internal control effectiveness. Management may wish to do the same if they believe significant deficiencies or material weaknesses exist.

Internal control effectiveness must be measured against defined criteria and not against subjective auditor driven opinions of deficiencies and weaknesses.

Examples must include sample of reporting against criteria of risk and control.

19. Is it necessary for the auditor to evaluate the severity of all identified internal control deficiencies?

Response: No.

It is necessary for management to evaluate the severity of all identified internal control deficiencies.

It is appropriate for the auditor to review management's process for doing so as part of their evaluation of management's assertions on internal control over financial reporting.

CARD[®] decisions' Response to PCAOB

20. Is it appropriate to require the auditor to communicate all internal control deficiencies (not just material weaknesses and significant deficiencies) to management in writing?

Response: Yes.

It is the responsibility of management to report all disclosure risks and internal control deficiencies (not just material weaknesses and significant deficiencies, however defined) to the auditor.

It is not intellectually possible for management to form an opinion on internal control effectiveness over financial reporting without knowing the deficiencies that are being accepted. Effective control can be defined as an acceptable level of deficiencies related to external financial disclosure. It stands to reason that they must be known and assessed to be responsibly considered acceptable by management.

The completeness and detail with which management reports disclosure risks and internal control deficiencies is a measure of the quality of their assertions on control effectiveness over financial reporting.

If the auditor finds additional deficiencies not reported by management, they must be reported to management and management's process for evaluating control effectiveness adjusted.

Auditors must take into account any deficiencies they find that were not reported by management in forming their opinion on the reliability of managements assertion on control effectiveness.

21. Are the matters that the Board has classified as strong indicators that a material weakness in internal control exists appropriately classified as such?

Response: Yes.

These indicators would contradict any management assertion that internal control over financial reporting is effective.

22. Is it appropriate to require the auditors to evaluate the effectiveness of the audit committee's oversight of the company's external financial reporting and internal control over financial reporting?

Response: No.

Management should consider the role of the Board during their self-assessment of internal control over financial reporting. External auditors are hired by the audit

CARD[®] decisions' Response to PCAOB

committee. Reporting on their employer's competence directly is an inherent conflict of interest.

Criteria are required to assess the role and reliability of the Board in assessing control over financial reporting.

23. Will auditors be able to effectively carry out their responsibility to evaluate the effectiveness of the audit committee's oversight?

Response: No.

It is difficult to believe auditors, appointed by the Board, remunerated by the Board and evaluated themselves by the Board, could be considered credible in forming an opinion on the audit committee's oversight. This section, if it stands, will almost certainly cause external auditors to give unreliable opinions.

24. If the auditor concludes that ineffective audit committee oversight is a material weakness, rather than require the auditor to issue an adverse opinion with regard to the effectiveness of the internal control over financial reporting, should the standard require the auditor to withdraw from the audit engagement?

Response: Yes.

Questions regarding forming an opinion and reporting:

25. Is it appropriate that the existence of a material weakness would require the auditor to express an adverse conclusion about the effectiveness of the company's internal control over financial reporting, consistent with the required reporting model for management?

Response: No.

Management may disclose a material weakness yet still provide reliable support for financial disclosures through other means.

If internal control is evaluated against defined criteria and given a score this question becomes irrelevant. It is possible for a company to be assigned an extremely low score against a set of defined criteria. Investors, regulators and other stakeholders may be guided accordingly.

Similarly, it is possible for a company to report huge losses, even to enter bankruptcy, while conforming to GAAP.

CARD[®] decisions' Response to PCAOB

26. Are there circumstances where a qualified "except for" conclusion would be appropriate?

Response: No.

Internal control effectiveness should be scored against predefined criteria. Direct opinions on internal control effectiveness are extremely subjective and have proven to be of limited value.

27. Do you agree with the position that when the auditor issues a nonstandard opinion, such as an adverse opinion, that the auditor's opinion should speak directly to the effectiveness of the internal control over financial reporting rather than to whether management's assessment is fairly stated?

Response: No, for all the reasons cited in our other responses.

Questions regarding auditor independence:

28. Should the Board provide specific guidance on independence and internal control-related non-audit services in the context of this proposed standard?

Response: Yes.

29. Are there any specific internal control-related non-audit services the auditor should be prohibited from providing to an audit client?

Response: Yes.

If the auditor is providing an opinion on management's assertions on internal control effectiveness, it is difficult to see how the auditor can be independent if they provide any internal control-related services or play a significant role in producing any of the external disclosures including tax provisions, deferred tax balances and many others.

The question might better be "Are there any specific internal control-related non audit services a client should be permitted to obtain from their auditor?"

Many external auditors play a significant role in determining a client's tax provision and interpreting generally accepted accounting principles. This is an inherent conflict.

Many auditors play a significant role advising on interpretation of GAAP or on appropriate financial disclosure. These roles have an inherent conflict.

Surveys indicate a high percentage of companies (40% to 50%) select control

CARD[®] decisions' Response to PCAOB

assessment software recommended or provided "free" by their auditor. Auditors have a huge influence on companies internal control frameworks when they recommend software or propose "best practice" controls or control checklists.

These represent significant inherent conflicts, particularly when providing an opinion on the reliability of management's assertions on internal control effectiveness.

Questions regarding auditor's responsibilities with regard to management's certifications:

30. Are the auditor's differing levels of responsibility as they relate to management's quarterly certifications versus the annual (fourth quarter) certification, appropriate?

Response: Yes.

31. Is the scope of the auditor's responsibility for quarterly disclosures about the internal control over financial reporting appropriate?

Response: Yes.

Professional Profile

Bruce W. McCuaig, B.Comm., CA-CIA, CCSA

Bruce McCuaig joined CARD[®] *decisions* in 1995. Prior to joining CARD[®] *decisions* Bruce held senior executive positions with Gulf Canada in Calgary and Toronto and Gulf Oil Corporation in Houston, Texas. While General Auditor of Gulf Canada Resources in 1987, Bruce implemented the original work team self-assessment concepts, including development of officer and board level presentations outlining the benefits of this new approach. He directed the first series of CSA pilots conducted during the summer of 1987 presented by Tim Leech and Paul Makosz.

Bruce's experience includes extensive audit and financial management in the oil and gas industry, both upstream and downstream, as well as exposure to the mining and banking sectors.

Since joining the firm in 1995 Bruce has worked with clients around the world training and overseeing complex, innovative Enterprise Risk & Assurance Management ("ERAM"), Control & Risk Self Assessment ("CRSA"), and Collaborative Assurance & Risk Design ("CARD[®] ") implementation initiatives in public and private sector clients ranging in size from individual departments to some of the world's largest multi-national corporations.

Bruce is an experienced speaker, author and presenter, participating regularly in international conferences on the subject of control self-assessment and publishing in professional audit and financial journals.

Some of Bruce's specific experiences and achievements include:

- General Auditor of Gulf Canada from 1983 to 1988 with responsibility for directing over 80 professional staff.
- Pioneering the use of a conceptual control framework for training, assessment and reporting purposes in Gulf Canada in the fall of 1986.
- Co-authoring a technical response to the Treadway Commission exposure draft in 1986 outlining the benefits of control self-assessment and the use of a control model for training and reporting.
- Co-authoring two important articles on Gulf's initial experience with and learnings from the control self assessment experience: "Is Everything Under Control? A New Approach to Corporate Governance", McCuaig/Makosz, Financial Executive Magazine, January/February, 1990 and "Ripe for a Renaissance", McCuaig/Makosz, Internal Auditor Magazine, December, 1990.
- Winner of Internal Auditor Magazine's Outstanding Contributor Award for 1990.
- Frequent speaker at IIA Conferences, Control Assessment Conferences and Government/Industry Associations.
- Hands-on experience assisting clients with complex enterprise risk management and enterprise risk implementations in large client organizations.
- Training and consulting for public and private sector staff in Canada, the U.S., the U.K., Holland, Greece, Australia, New Zealand, Malaysia, Hong Kong, the Middle East and Africa.
- Wrote "The Genesis of CSA", CSA Sentinel, May 1997 and "Audit, Assurance and CSA", Internal Auditor Magazine, June 1998.
- Co-authored "CRSA Current State of the Art, Its Origins and Impacts" published in Control Self-Assessment for Risk Management and Other Practical Applications published by John Wiley & Sons.

Professional Profile

Tim J. Leech, FCA·CIA, CCSA, CFE, MBA

Tim J. Leech is the founder and President of CARD[®] *decisions* Inc. based in Mississauga, Ontario, Canada. Previously, Tim was the Managing Director of the Canadian subsidiary of Network Security Management Ltd., part of the Hambros Bank group of companies headquartered in London, England. He also served as Director - Control & Risk Management Services with The Coopers & Lybrand Consulting Group in Toronto after a varied career with Gulf Canada in Toronto and Calgary. He holds a Master in Business Administration degree majored in human resources and was elected Fellow of the Institute of Chartered Accountants in recognition of distinguished service to the profession.

Leech's practice includes enterprise-wide risk and assurance management; Collaborative Assurance & Risk Design[™] ("CARD[®]") software development, training and consulting; control and risk self-assessment ("CRSA") training and implementation services; specialized litigation support services; business ethics advisory services; internal audit training and consulting; and control/risk governance consulting services. He has provided training for public and private sector staff located in Canada, the U.S., the European Community, Australia, South America, Africa and the Middle and Far East. Leech has received worldwide recognition as a pioneer in the fields of enterprise risk and assurance management, Collaborative Assurance and Risk Design, and control and risk self-assessment.

Some of Leech's experiences and achievements include:

- pioneering and developing a work team driven approach to control and risk management and reporting that has been recognized globally as a leading edge, control and risk management tool;
- developing Collaborative Assurance and Risk Design[™] training methods and software used by major organizations around the world. Some of the organizations that have acquired licences over the past decade to use CARD[®] training tools internally include: BellSouth, British Gas, Shell U.K., Georgia-Pacific, NatWest Bank, University of California, CIBC, Mobil, Cabot Corporation, Ansett Airlines, TD Bank, NorthEast Utilities, Chiquita Brands, Compart, City of Detroit, Telephone and Data Systems, Telstra, Western Mining, Canada Life, and Australian Taxation Office;
- numerous T.V. appearances, a national radio show, and a monthly column on control, ethics, and fraud related topics;
- authoring technical papers in response to exposure drafts of control governance studies in the U.S., the U.K., and Canada including reports by the Treadway Commission, COSO, Cadbury, and CoCo internal control research projects and the new standards exposure from the IIA;
- developing technical material for research studies on CSA/CRSA including the IIA report CSA: Making the Choice, the IIA research study CSA: Experience, Current Thinking and Best Practices and a text published by John Wiley titled "Control Self-Assessment for Risk Management and Other Practical Applications";
- delivery of expert witness services and testimony during civil and criminal actions related to fraud, secret commissions, conflict of interest, breach of contract, and officer/director due diligence;
- developing training tools that have proven effective in a wide range of nationalities and cultures. Training on CARD[®] methods and tools is available in English, Spanish, German, Dutch, French, and Italian through Oxley Fitzpatrick in the U.K., Rosés Auditores in Spain, and participating KPMG offices located around the world;
- member of the I.I.A. Enterprise Risk & Self-Assessment Advisory Panel and author of the IIA CCSA practice exam; and
- primary author and developer of CARD[®] *map* software - the world's first Collaborative Assurance and Risk Design[™] groupware. CARD[®] *map* software is used by major companies and public sector organizations around the world.