CANADIAN BANKERS ASSOCIATION

Box 348, Commerce Court West
199 Bay Street, 30th Floor
Toronto, Ontario, Canada M5L 1G2
www.cba.ca

Karen Michell
Vice-President, Banking Operations
Tel: (416) 362-6093 Ext. 335
Fax: (416) 362-0563
kmichell@cba.ca

September 7, 2006

Sent via e-mail to rule-comments@sec.gov

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

Dear Ms. Morris:

Re: Subject File S7-11-06 - Concept Release

The Canadian Bankers Association ("CBA") welcomes the opportunity to provide comments on the concept paper released by the Securities and Exchange Commission pursuant to the Commission's intention to provide management guidance regarding its evaluation and assessment of internal controls over financial reporting as required by the Sarbanes-Oxley Act of 2002 ("SOX" or "the Act").

The CBA is a professional industry association that provides information, advocacy, education and operational support services to its members, the 54 chartered banks of Canada, which include domestic banks, foreign banks and branches of foreign banks. The CBA's mission is to be a leading contributor in the development of public policy on issues that affect the financial services sector. A number of CBA members are foreign private issuers and are subject to the requirements of SOX 404, as well as equivalent draft requirements of the Canadian Securities Administrators ("CSA").

Our overall view is in line with the Commission's in that we agree that a single methodology that meets the needs of every company is not practical. Principles-based guidance is the most feasible approach to adopt. The guidance should be specific but not so prescriptive as to preclude the use of professional judgment in its application. We understand that this balance is difficult to achieve but we encourage the SEC to favour judgment over presciptiveness in those situations where the balance may be difficult to achieve otherwise.

In the absence of guidance the approach outlined in PCAOB Auditing Standard No. 2 (AS2) has become the de facto standard for management's assessment. Therefore, it is critical that any new guidance for management be aligned and consistent with any changes to AS2. While the independent auditors may have a different objective when assessing internal controls over financial reporting, management and the auditors need to work together to ensure that the most effective and efficient audit is carried out with appropriate reliance being placed on the work

Appendix 1

General

1. Would additional guidance to management on how to evaluate the effectiveness of a company's internal control over financial reporting be useful? If so, would additional guidance be useful to all reporting companies subject to the Section 404 requirements or only to a sub-group of companies? What are the potential limitations to developing guidance that can be applied by most or all reporting companies subject to the Section 404 requirements?

Yes, additional principles-based guidance would be useful in some areas such as:

- Entity-level controls - Further clarification of the linkage between entity-level controls and processes and potential leverage of entity-level controls to assess individual processes and to perform an effective top-down evaluation is necessary. The guidance must be aligned with AS2 changes.

- Baselining - there is a need further clarification on assessing operating effectiveness of IT application controls. An informal practice of "baselining" once every three years has emerged. This practice, however, has not been formalized and publicly endorsed by the SEC.

- Disclosure of material changes in internal control - Further clarification on what constitutes 'material' is needed.

Guidance should be generic, but should allow for some flexibility based on parameters to be defined by the SEC (e.g., size of assets, revenues, etc.). The guidance should provide a reasonable framework within which to operate, but should not be so prescriptive as to limit the exercise of management's judgment. Coordination between the PCAOB and the SEC is critical to avoid situations in which the PCAOB may provide rules that would restrict interpretation of the principles-based guidance.

2. Are there special issues applicable to foreign private issuers that the Commission should consider in developing guidance to management on how to evaluate the effectiveness of a company's internal control over financial reporting? If so, what are these? Are such considerations applicable to all foreign private issuers or only to a sub-group of these filers?

As a result of stringent regulatory supervision of banks in Canada that already ensures the ongoing safety and soundness of our operations, banks have internal control and compliance frameworks in place. In addition, CBA members are subject to other regulatory requirements, such as Basel II and Legislative Compliance Management. The underlying foundation of these governance frameworks is often similar. CBA believes that there should be more opportunity to streamline SOX 404 requirements for organizations in highly-regulated industries.

In addition, for the banking industry, the magnitude of the ending balances in the financial statements do not directly reflect that the underlying processes may be lower risk due to high volumes but low individual values with very routine transaction processing controls. Consideration should be given to this situation.

In the area of outsourcing, many Canadian banks with October 31 year-ends receive SAS 70 reports from U.S. suppliers with December 31 year-ends. The timing issue has resulted in the banks' external auditors placing little to no reliance on the SAS 70 reports as they pertain mostly to a prior year, and therefore there is additional work for Canadian banks to evaluate those controls residing at the U.S. suppliers. In this regard, we request guidance regarding considerations under which such a SAS 70 report can be deemed relevant to the current year under evaluation, particularly where such a report has been provided annually with no major issues. In addition, we request guidance regarding alternative options/approaches for management to evaluate internal controls residing at an outsourcing supplier, to supplement reliance on the SAS 70 or other equivalent reports. These options/approaches should be aligned with any changes to AS2.

3. Should additional guidance be limited to articulation of broad principles or should it be more detailed?

As indicated above, the guidance should provide a reasonable framework of broad principles within which to operate, but should not be so prescriptive as to limit the exercise of management's judgment.

4. Are there additional topics, beyond what is addressed in this Concept Release, that the Commission should consider issuing guidance on? If so, what are those topics?

No additional topics have been identified.

5. Would additional guidance in the format of a Commission rule be preferable to interpretive guidance? Why or why not?

We believe interpretive guidance would provide the greatest flexibility to filers.

6. What types of evaluation approaches have managements of accelerated filers found most effective and efficient in assessing internal control over financial reporting? What approaches have not worked, and why?

Our member banks have generally implemented a top-down risk-based approach on the strength of entity-level controls, and based on our assessment of inherent risk. Based on the risk ranking, the banks have varied the nature, timing and extent of their tests of operating effectiveness.

7. Are there potential drawbacks to or other concerns about providing additional guidance that the Commission should consider? If so, what are they? How might those drawbacks or other concerns best be mitigated? Would more detailed Commission guidance hamper future efforts by others in this area?

The Commission should consider that guidance to management must be consistent with the principles of AS2, but provide adequate flexibility within which to exercise management's judgment.

8. Why have the majority of companies who have completed an assessment, domestic and foreign, selected the COSO framework rather than one of the other frameworks available, such as the Turnbull Report? Is it due to a lack of awareness, knowledge, training, pressure from auditors, or some other reason? Would companies benefit from the development of additional frameworks?

The COSO framework is an internationally recognized methodology that has been practical to implement. With so many accelerated filers adopting COSO, we do not believe the development of additional frameworks would be of particular value.

9. Should the guidance incorporate the May 16, 2005 "Staff Statement on Management's Report on Internal Control Over Financial Reporting" (Staff Statement)? Should any portions of the May 16, 2005 guidance be modified or eliminated? Are there additional topics that the guidance should address that were not addressed by that statement? For example, are there any topics in the staff's "Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports Frequently Asked Questions (revised October 6, 2004)"19 that should be incorporated into any guidance the Commission might issue?

We believe that the Staff Statement was useful in confirming the principles advocated by the Commission. Further clarification is required regarding:

- the implementation of a top-down risk-based approach and scope and timing of testing and assessment;

- The factors that should be used in assessing the significance of deficiencies evaluating internal control deficiencies, i.e. what constitutes a significant deficiency and material weakness;

- The ability to use the previous year's conclusions on design and operating effectiveness to reduce the amount of review and testing of processes and controls in subsequent periods.

10. We also seek input on the appropriate role of outside auditors in connection with the management assessment required by Section 404(a) of Sarbanes-Oxley, and on the manner in which outside auditors provide the attestation required by Section 404(b). Should possible alternatives to the current approach be considered and if so, what? Would these alternatives provide investors with similar benefits without the same level of cost? How would these alternatives work?

Further clarification should be provided to auditors to encourage the use or reliance on the work of management to make more efficient use of their own time in performing their audits of internal control. In addition, reliance on a properly constituted Internal Audit function operating in accordance with the professional practices of the Institute of Internal Auditors to confirm management's certification should be promoted.

CBA members believe that the SEC and PCAOB should also assess the feasibility of eliminating the auditor attestation requirement, or alternatively introduce a rotational cycle for attestation (for example, every 3 years) or a limited risk-based or specified attestation. In Canada, the Canadian Securities Administrators (CSA) have elected to monitor management's compliance with the process and to consider audit requirements in the future based on the findings of their

monitoring process. The CSA has also reflected that this does not preclude the board of directors or the audit committees from engaging the auditors to perform specified work.

We would support removing the external auditor's opinion on management's assessment process. The capital markets need assurance that internal controls over financial reporting are well-designed and operating effectively, and this can be achieved without focusing audit attention on management's process, but rather on management's conclusion.

Risk and Control Identification

11. What guidance is needed to help management implement a "top-down, risk-based" approach to identifying risks to reliable financial reporting and the related internal controls?

Further clarification is required on the nature and extent of linkage between entity level controls and processes, and potential leverage of entity-level controls to assess individual processes. Guidance around opportunities to reduce or eliminate testing of medium and low risk controls/processes would be particularly useful.

12. Does the existing guidance, which has been used by management of accelerated filers, provide sufficient information regarding the identification of controls that address the risks of material misstatement? Would additional guidance on identifying controls that address these risks be helpful?

While guidance on general types of controls has been useful, companies have tended to evaluate more controls than perhaps necessary to address the risk of material misstatement. Most CBA members believe that the evaluation should be limited to appropriate entity level controls, including general IT controls, period-end financial reporting processes, core finance processes and other non-routine judgment-based processes such as acquisitions, divestitures and key provisioning processes. Guidance should be provided in these areas to focus the evaluation process as well as identifying those areas, such as low risk controls/processes, where evaluations could be reduced or possibly eliminated.

13. In light of the forthcoming COSO guidance for smaller public companies, what additional guidance is necessary on risk assessment or the identification of controls that address the risks?

Further guidance on integrating the following considerations into the risk assessment is required:

- Fraud;
- end-user computing/spreadsheets.

14. In areas where companies identified significant start-up efforts in the first year (e.g., documentation of the design of controls and remediation of deficiencies) will the COSO guidance for smaller public companies adequately assist companies that have not yet complied with Section 404 to efficiently and effectively conduct a risk assessment and identify controls that address the risks? Are there areas that have not yet been addressed or need further emphasis?

Question not applicable to CBA members.

15. What guidance is needed about the role of entity-level controls in evaluating and assessing the effectiveness of internal control over financial reporting? What specific entity-level control issues should be addressed (e.g., GAAP expertise, the role of the audit committee, using entity-level controls rather than low-level account and transactional controls)? Should these issues be addressed differently for larger companies and smaller companies?

There is a need for principles-based guidance on how to evaluate entity-level controls and interpret the results thereof to determine the impact on financial reporting. Some examples of specific entity-level controls that warrant this guidance are the Code of Business Conduct, Organizational Structure, HR policies and procedures and Risk Management policies. It is difficult to show a direct link to financial reporting for these processes and demonstrate their effectiveness in reducing the risk of material misstatement.

The principles of 'tone at the top' should be the same for larger and smaller companies. Where one control may not be as structured or in place in smaller companies, another entity-level control or controls must operate to mitigate the risks to financial reporting.

16. Should guidance be given about the appropriateness of and extent to which quantitative and qualitative factors, such as likelihood of an error, should be used when assessing risks and identifying controls for the entity? If so, what factors should be addressed in the guidance? If so, how should that guidance reflect the special characteristics and needs of smaller public companies?

Principles-based guidance should be given on:

- What could constitute a high, moderate or low risk of 'material' misstatement.
- Determining relevant financial reporting assertions. Evaluations should not necessarily cover the end-to-end process, but rather should be focused on the controls necessary to achieve the financial reporting assertions and control objectives that have a reasonable bearing as to whether accounts are fairly stated.

17. Should the Commission provide management with guidance about fraud controls? If so, what type of guidance? Is there existing private sector guidance that companies have found useful in this area? For example, have companies found the 2002 guidance issued by the AICPA Fraud Task Force entitled "Management Antifraud Programs and Controls"23 useful in assessing these risks and controls?

Generally, principles-based guidance is required on how "deep" to go with fraud controls and also to limit the scope to the risk of financial reporting fraud. In addition, more guidance is required on the evaluation of the risk of management override. Other than high-level control environment-type controls, very often, there are no controls that directly address this risk in an organization.

Many of the large accounting firms have issued a whitepaper on the subject of fraud controls, which has been useful.

18. Should guidance be issued to help companies with multiple locations or business units to understand how those affect their risk assessment and control identification activities? How are companies currently determining which locations or units to test?

This is definitely an area of concern for companies in multiple locations and across geographic borders. Some factors to consider are:

- degree of centralization and homogeneity of the controls in multiple locations;
- entity level controls that support the homogeneity of the processes and controls in multiple locations (e.g.; training, policy and procedure manuals, job descriptions, oversight and monitoring controls, etc).

Based on the above considerations, we recommend that the SEC provide principles-based guidance on the following determinations:

- extent to which entity level controls can be relied upon to determine the homogeneity across locations. On what basis can like controls in multiple locations be pooled to reduce the testing in all locations?
- sample size in each location.

Management's Evaluation

19. What type of guidance would help explain how entity-level controls can reduce or eliminate the need for testing at the individual account or transaction level? If applicable, please provide specific examples of types of entity-level controls that have been useful in reducing testing elsewhere.

Principles-based guidance on the evaluation of entity level processes as a whole is required. Very often, entity level processes are evaluated individually without regard to the interdependency and interplay of these processes to achieve an overall effective control environment.

Principles-based guidance is also needed on what constitutes effective analytics and monitoring in entity-level controls. In general, the following entity-level controls can be linked to the evaluation of process/transaction specific controls:

- Accounting Policy
- Financial Analysis
- Whistleblower Policies

20. Would guidance on how management's assessment can be based on evidence other than that derived from separate evaluation-type testing of controls, such as on-going monitoring activities, be useful? What are some of the sources of evidence that companies find most useful in ongoing monitoring of control effectiveness? Would guidance be useful about how management's daily interaction with controls can be used to support its assessment?

Provide principles-based guidance on how companies can leverage other governance functions or activities in the organization, e.g. Operational Risk Management, Risk and Control Self Assessment, Basel II and Internal Audit, to support or augment their evaluation. Organizations such as banks with robust internal audit functions should be able to leverage the results of internal audit mandate work to allow them to conclude on the internal controls without the need for extensive specific testing. Internal Audit mandates require an opinion on all aspects of internal controls, including internal controls over financial reporting.

If companies are able to leverage the work of other governance functions in the organization, provide guidance on what documentation would be required to evidence this.

21. What considerations are appropriate to ensure that the guidance is responsive to the special characteristics of entity-level controls and management at smaller public companies? What type of guidance would be useful to small public companies with regard to those areas?

Question not applicable to CBA members.

22. In situations where management determines that separate evaluation-type testing is necessary, what type of additional guidance to assist management in varying the nature and extent of the evaluation procedures supporting its assessment would be helpful? Would guidance be useful on how risk, materiality, attributes of the controls themselves, and other factors play a role in the judgments about when to use separate evaluations versus relying on ongoing monitoring activities?

CBA members believe that the SEC and PCAOB should reconsider the approach for evaluation of internal controls over financial reporting to focus only on areas of risk of material misstatement. Evaluation that is targeted to areas of greater likelihood of material misstatements is likely to be more valuable and sustainable.

Most members believe that the evaluation should be limited to appropriate entity level controls, including general IT controls, period-end financial reporting processes, core finance processes and other non-routine judgment-based processes such as acquisitions, divestitures and key provisioning processes.

In addition, CBA believes that some testing relief should be provided by giving consideration to rotational testing in low and medium risk areas. In particular, routine transactions of low value but high volume could be assessed periodically through rotational testing. This rotational testing can also include a benchmarking strategy in areas such as IT application controls and in standardized processes where no changes have occurred. Guidance is required in this area.

23. Would guidance be useful on the timing of management testing of controls and the need to update evidence and conclusions from prior testing to the assessment "as of" date?

We would like principles-based guidance on the timing of controls testing and, more importantly, guidance on the requirements to update testing by the end of the year. We see a requirement for principles-based guidance on being able to leverage the continuous nature of controls within

organizations to reduce or eliminate substantial retesting efforts at or around year-end, when there is very limited time. Principles need to recognize that control monitoring and testing is a continuous process; "roll forward testing" toward year end is an unnecessary incremental assessment step.

24. What type of guidance would be appropriate regarding the evaluation of identified internal control deficiencies? Are there particular issues in evaluating deficient controls that have only an indirect relationship to a specific financial statement account or disclosure? If so, what are some of the key considerations currently being used when evaluating the control deficiency?

- Principles-based guidance on the definitions of 'likelihood' (remote and reasonably possible) and 'magnitude' (inconsequential, more than inconsequential, and material) is needed. In addition, guidance on the following areas would be helpful:

- Quantification of the impact of a deficiency, in particular, the potential impact and its relevance in the classification of a deficiency;

- Aggregation of a group of like deficiencies. Guidance on the bases under which deficiencies should be aggregated would be useful i.e. should we aggregate based on financial statement captions, themes, assertions etc…?;

- Impact of compensating controls;

- Qualitative considerations in deficiency assessment.

25. Would guidance be helpful regarding the definitions of the terms "material weakness" and "significant deficiency"? If so, please explain any issues that should be addressed in the guidance.

Provide principles-based guidance on those factors that should be used to establish the parameters by which deficiencies are classified. Please also see our comments to question number 24.

26. Would guidance be useful on factors that management should consider in determining whether management could conclude that no material weakness in internal control over financial reporting exists despite the discovery of a need to correct a financial statement error as part of the financial statement close process? If so, please explain.

Yes, there is a need to differentiate between a control weakness and an error that was identified through the operation of the control.

27. Would guidance be useful in addressing the circumstances under which a restatement of previously reported financial information would not lead to the conclusion that a material weakness exists in the company's internal control over financial reporting?

Not all re-statements point to a weakness in internal controls over financial reporting. GAAP changes may result in the restatement of prior periods for comparability with the current period.

Principles-based guidance on considerations to support the conclusion of a material weakness is needed, such as:

- Extent to which misstatement masks a change in earnings or key performance ratings;
- Whether the misstatement has the effect of increasing management's compensation;
- Whether the misstatement involves concealment of a transaction that is unlawful, or in violation of a regulatory or contractual requirement.

28. How have companies been able to use technology to gain efficiency in evaluating the effectiveness of internal controls (e.g., by automating the effectiveness testing of automated controls or through benchmarking strategies)?

Technology has not been used widely by CBA members to assist the evaluation, other than through the use of efficiency tools such as automated repositories. We expect this will improve as experience is gained in subsequent years.

29. Is guidance needed to help companies determine which IT general controls should be tested? How are companies determining which IT general controls could impact IT application controls directly related to the preparation of financial statements?

We believe that much greater clarity is required on the testing requirements for IT general controls. Most members are erring on the side of caution and are including the majority of IT general controls in the scope of their testing. We see the need for principles-based guidance on the following:

- identifying relevant financial reporting related control objectives that may be associated with IT general controls;
- the acceptance of the pooling concept and the considerations to be used when pooling general controls to reduce the scope of IT general controls testing;
- establishing the impact of IT general control deficiencies on financial reporting.

30. Has management generally been utilizing proprietary IT frameworks as a guide in conducting the IT portion of their assessments? If so, which frameworks? Which components of those frameworks have been particularly useful? Which components of those frameworks go beyond the objectives of reliable financial reporting?

Some companies are using 'Control Objectives for Information and Related Technology' (COBIT) as an IT governance framework. The COBIT framework is very detailed and has to be scoped to focus on IT controls that support the integrity of financial applications.

Documentation to Support the Assessment

31. Were the levels of documentation performed by management in the initial years of completing the assessment beyond what was needed to identify controls for testing? If so, why (e.g., business reasons, auditor required, or unsure about "key" controls)? Would

specific guidance help companies avoid this issue in the future? If so, what factors should be considered?

There is a belief among members that documentation levels are beyond what is needed to identify controls for testing. We believe that this is due to a lack of guidance causing management and audit firms to interpret the legislation too broadly. We believe that principles-based guidance is required on the level of documentation needed to support:

- the operation of controls;
- tests of operating effectiveness;
- user acceptance testing (UAT).

In addition, principles-based guidance is required on the retention period for:

- the evaluation work and related results;
- underlying source documents and/or transaction records.

Section 802 of the Sarbanes-Oxley Act requires the external auditors to maintain documentation of their audit or review work for seven years, during which time their work papers could be inspected by the SEC. Require clarification on whether this retention period applies to the documentation of management's assessment.

32. What guidance is needed about the form, nature, and extent of documentation that management must maintain as evidence for its assessment of risks to financial reporting and control identification? Are there certain factors to consider in making judgments about the nature and extent of documentation (e.g., entity factors, process, or account complexity factors)? If so, what are they?

Same principles-based guidance as outlined to question 31.

33. What guidance is needed about the extent of documentation that management must maintain about its evaluation procedures that support its annual assessment of internal control over financial reporting?

Same principles-based guidance as outlined to question 31.

34. Is guidance needed about documentation for information technology controls? If so, is guidance needed for both documentation of the controls and documentation of the testing for the assessment?

Guidance on the controls related to in scope End User Computing applications, their risk assessment and evidence required for both implementation and testing of application controls would be helpful.

35. How might guidance be helpful in addressing the flexibility and cost containment needs of smaller public companies? What guidance is appropriate for smaller public companies with regard to documentation?

Question not applicable to CBA members.

performed by others. We have provided our detailed views regarding the appropriate role of outside auditors in our response to question 10 from the concept release document.

Attached as Appendix 1 are our comments on each of the questions posed in the concept release document.

The CBA and its members look forward to reviewing the principles-based guidance that is expected to ultimately emerge from this consultation process and commend the Commission for its positive response to stakeholders' previous feedback through the roundtable and comment letter forum.

Please do not hesitate to contact us if you wish to discuss these comments further.

Sincerely,