September 15, 2006

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

RE: File Number S7-11-06 "Concept Release Concerning Management's Reports on Internal Control over Financial Reporting"

Dear Ms. Morris:

The Institute of Management Accountants (IMA) is pleased to submit to the SEC the attached **"A Global Perspective on Assessing Internal Control Over Financial Reporting"** in response to the SEC's May 2006 Concept Release Concerning Management's Reports on Internal Control over Financial Reporting.

It is important to note that the IMA is not providing specific responses to the 35 questions you pose in the Concept Release. However, this Discussion Draft does offer a practical, principles- and risk-based solution to what we see as a global issue: the reliability of financial disclosures. We believe this is a solution that reduces cost for enterprises of all sizes, increases the overall benefits of management's compliance efforts and reduces the incremental external audit liability embedded in the current SOX rules. The assessment guidance we propose is "controls framework neutral" and places more responsibility in the hands of management for risk and controls self-assessments.

IMA's Financial Reporting Committee (FRC) has submitted a separate comment letter addressing many of the 35 questions contained in the Concept Release.

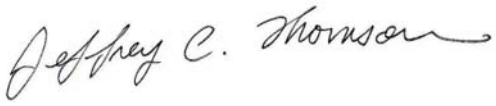
Key characteristics of the IMA draft global assessment guidance draft include:

- It is **written with a management focus** and draws on decades of practical field experience implementing risk and control self-assessment systems globally, findings of FEI's research study on SOX control deficiency reporting, and a landmark IMA research study on the root cause challenges with the current implementation regulations (study to be released by the IMA later this month). IMA is releasing this draft for critical public comment coincident with this filing (comments due by November 18) to further assist the SEC as it moves forward in developing management assessment guidance.

- It **reflects advances in the global risk and quality management fields that have occurred over the past 25 years** in the spirit of developing a true "top-down, risk-based approach" to lower compliance costs and help ensure the continued leadership of U.S. capital markets.
- It **addresses many of the current "pain points" experienced by SOX practitioners** with a particular emphasis on identifying assessment flexibility options and cost reduction opportunities**.**
- It **provides a global perspective and encourages the harmonization of control assessment frameworks in line with SEC requests** in the Concept Release (e.g., footnote 8 on page 7 – "we encourage companies to examine and select a framework that may be useful in their own circumstances and the further development of alternative frameworks"). To this end, IMA's draft guidance document demonstrates how to "treat risks" relative to the existing COSO and COSO linked frameworks, as well as Canadian, U.K., IT security and ethics focused control criteria.
- It **provides an assessment framework that, in addition to its applicability to ICoFR, can also be used to assess internal control on <u>any</u> dimension of enterprise risk and operational risk management,** including product quality, customer service, continuity of operations, IT security, physical security, terrorist vulnerability, cost optimization, general compliance and other practical business contexts. An assessment framework that has the ability to address broader business applications (not just ICoFR) helps foster acceptance by work units, and helps improve the "ROI" from an organization's overall compliance program.

Thank you for the opportunity. The IMA stands ready to meet with the SEC at its convenience in a work session or other forum to discuss the specifics of the risk-based management assessment guidance we are proposing in draft form.

Paul Sharman, ACMA
President & CEO
Institute of Management Accountants
201-474-1579 psharman@imanet.org



Jeffrey C. Thomson
Vice President, Research and Applications Development
Institute of Management Accountants
201-474-1586 jthomson@imanet.org

TO POST COMMENTS ON IMA'S DRAFT GLOBAL ASSESSMENT GUIDANCE, SEND TO <u>ICoFRComments@imanet.org</u> by November 18, 2006.

A GLOBAL PERSPECTIVE ON ASSESSING INTERNAL CONTROL OVER FINANCIAL REPORTING

("ICoFR")

DISCUSSION DRAFT FOR COMMENT*

Development Led By:
Institute of Management Accountants

* The following organizations have agreed to review and critically evaluate this draft: American Electronics Association (AeA), American Society for Quality (ASQ), Association of Government Accountants (AGA), Open Compliance and Ethics Group (OCEG), and a number of highly experienced individuals. Invitations to comment have been extended by the IMA to a wide range of organizations with an interest in the subject.

September 2006

A GLOBAL PERSPECTIVE ON ASSESSING ICOFR
TABLE OF CONTENTS

15/09/2006

A GLOBAL PERSPECTIVE ON ASSESSING ICOFR
TABLE OF CONTENTS

ATTACHMENTS

EXECUTIVE SUMMARY

This IMA led and funded discussion paper has been written in direct response to the SEC's request for public input on how management should tackle the task of assessing and reporting on the state of internal control over financial reporting for SOX. In addition to filing this paper with the SEC to generate productive debate and discussion, it will also be distributed to capital market security regulators in countries around the world, auditor oversight bodies, and interested professional associations and individuals for critical comment and feedback before being published in final form.

It is important to note that this paper does not propose minor, incremental "tweaks" to the current SOX ICoFR regulatory process. While our suggestions are certainly not modest in their aspirations, we do believe they represent well researched, comprehensive and practical solutions to the current groundswell of concerns being raised. IMA believes these solutions take full account of the many advances over the past 30 years in the fields of risk management, quality and internal control.

The biggest challenge to meaningful change of the current SOX regulatory process, in our view, will ironically be the resistance to change in the larger companies that have already spent billions of dollars complying with the current SOX rules. More than a few large companies that have vigorously complained about the current SOX regime may fall back on a well-known adage – "better the devil we know than one we don't". With that said, companies large and small are still seeking improved guidance to lower costs and improve benefits which our proposal addresses head on.

This paper also analyzes the problems in the current SOX 302/404 regulatory set and proposes some tangible and practical ways to "rethink" and "reengineer" how the goals set by U.S. Congress in the Act can and should be tackled.

The key elements of IMA's proposed management assessment guidance are:

- A practical, risk-based approach that draws on risk standards around the globe. The language and approach are "management centric", not "auditor centric".
- An approach that draws on quality principles in terms of understanding process error rates as a key element of residual risk outcomes, as well as the criticality of measuring and monitoring process key performance indicators rather than primary emphasis on inspection after the fact.
- A risk assessment methodology that is "controls framework neutral" in the spirit of accelerating the move toward global harmonization of controls frameworks.
- An approach that puts an emphasis on "risk and controls self assessment" to put more accountability and responsibility in the hands of management relative to their external audit partners. Management in this context is not only internal auditors and controllers – also business process owners and personnel in business units who need to learn and apply the language of risk to truly determine "how much control is enough" to achieve reliable financial disclosures and protect shareholder interests.
- An approach that improves the management-external auditor partner relationship by suggesting the requirement to provide binary/yes-no conclusions on effectiveness of the system of ICoFR should be eliminated. These subjective determinations, which lead to costly disagreements on the number of "key" controls to be tested, should be replaced by consensus agreement on whether the residual risk that remains after the

initial control portfolio is applied is sufficient to achieve the goal of reliable account balances and notes disclosures.

As SEC Chairman Cox has said, it is not too late to get it right on SOX compliance. Incremental and entrenched thinking must be replaced by out-of-the box thinking to protect shareholder interests and improve the U.S. position in global capital markets. The IMA sincerely hopes that this paper helps achieve these critical goals.

TO POST COMMENTS ON IMA'S DRAFT GLOBAL ASSESSMENT GUIDANCE, SEND YOUR COMMENTS TO ICoFRComments@imanet.org or jthomson@imanet.org by November 18, 2006.

.

FORWARD

Section 404 of the Sarbanes-Oxley Act of 2002 ("SOX") calls for management to formally acknowledge accountability for internal control over financial reporting ("ICoFR"), provide an opinion on the effectiveness of those controls and, perhaps most importantly, requires each registrant's external auditor provide an opinion on management's control effectiveness assessment. Although this new law added a level of formality that hadn't previously existed and would most certainly entail higher compliance costs, few anticipated just how difficult and expensive it would actually turn out to be. Countries around the world looked on with interest at this new development in U.S. securities law and corporate governance.

On a positive note, The Sarbanes Oxley Act and the underlying legislation has produced many benefits to U.S. society, investors and publicly traded companies. The legislation has clearly put corporate executives "on notice" that fraudulent behavior is unacceptable and, most importantly, can result in severe consequences. Investors have more confidence that those serving as stewards for their investments are reporting in an ethical and transparent manner. Publicly traded companies have elevated the emphasis on the benefits of reliable internal control systems, sound ethics, and continuous process management. Unfortunately the negatives currently are overshadowing the positives.

Based on our research we believe SOX the law enacted by Congress is not the issue – the implementation guidance is. The central question is how to restore/enhance shareholder's confidence in the stewardship of their investments at a cost that is tolerable. The issue has global implications and this discussion draft addresses both U.S. "pain points" of SOX 404 implementation as well as global perspectives and implications highly relevant to the debate.

More than four years have passed since Sarbanes-Oxley Section 404 was enacted. The world now more fully understands just how difficult it is to create regulations and guidance that explain how to do what U.S. Congress asked for in 2002 at a cost that is palatable to society. The adequacy of the "how to" guidance available to management and external auditors of U.S. listed companies has been questioned and challenged by many public companies. The groundswell of complaints resulted in the Christopher Cox, Chairman of the SEC, formally acknowledging the problem on May 10, 2006:

> *Auditing Standard No. 2 gives guidance to independent auditors tasked with determining whether a company's internal controls are effective. No similar guidance, however, exists for companies and for their management. And in the absence of direction from us, companies have been basing the assessment of their controls on AS2.*

In a press release dated May 17, 2006 the SEC committed to positive steps to address this issue, including developing and issuing new assessment guidance for management. Chairman Cox stated:

> *By providing practical guidance to companies, by working with the Public Accounting Oversight Board on their forthcoming revised standards for auditors, and by examining how the PCAOB inspection process is succeeding in increasing the efficiency and cost-effectiveness of the audit process, we will*

take a giant step toward 'getting it right' when it comes to Section 404 compliance.

Other countries around the world, including Canada, the U.K., the European Union and others, have been carefully assessing the applicability of the U.S. "SOX experiment". To date, they have generally concluded that the path taken by the U.S. to date, while completely valid in its aspirations, is still too fraught with methodology and cost problems to consider imposing the same approach in their country.

The reality is that prior to SOX management and auditors, both internal and external, did not have robust methodology or the necessary training to arrive at fully supportable and, most importantly, repeatable conclusions on whether controls over external financial reporting in any given organization are, or are not, "effective". Progress developing new tools and techniques to accomplish this task has been painful, but much has already been accomplished, largely as a result of the massive global impact of this new law. Much still remains to be done to better understand the dynamics that cause material undetected errors in auditor certified financial statements.

On July 11, 2006 the SEC issued ***Concept Release, Request for Comment Concerning Management's Reports on Internal Control Over Financial Reporting*** to better understand the extent and nature of public interest in the development of additional guidance for management regarding its evaluation and assessment of internal control over financial reporting. The stated purpose of the July 2006 SEC Request for Comment is to ensure that the guidance the Commission develops addresses the needs and concerns of public companies, consistent with the protection of investors.

In recognition of the urgent need to provide the SEC with timely input this "Discussion Draft for Comment" is being filed with the SEC as a component of IMA's response to the July 11 Concept Release. It will also be simultaneously issued for comment and feedback to capital regulators around the world, knowledgeable and interested professionals through professional associations that have expressed interest in this project ("PARTICIPATING ORGANIZATIONS"), and to other interested and knowledgeable experts in the field via IMA invitations to comment ("PARTICIPATING INDIVIDUALS"), general press releases, and publicity on this project. Comments on this discussion paper should be addressed via post by November 18, 2006 to:

Jeffrey Thomson
VP Research & Applications Development
Institute of Management Accountants
10 Paragon Drive
Montvale, New Jersey
07645-1760

Or via e-mail to ICoFRComments@imanet.org

The IMA will use the comments and input received to revise this paper and issue a formal exposure draft for additional comment and revision. All comments received by the IMA in response to this paper will be posted for public review and academic research purposes.

AUTHORITY & ACKNOWLEDGEMENTS

When the SEC released final guidance for Section 404 they listed criteria for a "suitable framework" for use by registrants when assessing the effectiveness of controls over financial reporting. To qualify the SEC has stated that the framework must:

1. Be free from bias.
2. Permit reasonably consistent qualitative and quantitative measurements of a company's internal control.
3. Be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal controls are not omitted.
4. Be relevant to an evaluation of internal control over financial reporting.

In Canada, the Canadian Institute of Chartered Accountants expanded the definition by indicating that the framework must also be:

> *"understandable so it is not subject to significantly different interpretation by intended users."*

As a result of widespread complaints regarding the adequacy of current control assessment guidance and the methods currently being used, a number of organizations, including the SEC and COSO, have recognized the need for more practical and cost effective control assessment guidance and, over the longer term, the need to "globally harmonize" controls and assessment frameworks around the world. More specifically, in its July 11, 2006 Concept Release, the SEC acknowledged that the COSO 1992 controls framework, by itself, is not sufficiently complete to allow management to make consistent determinations on the current effectiveness of ICoFR:

> "While the COSO framework provides an integrated framework that identifies components and objectives of internal control, it does not set forth detailed guidance as to the steps that management must follow in assessing the effectiveness of a company's ICoFR. We, therefore, distinguish between the COSO framework and other forms of guidance that illustrate how to conduct an assessment of the effectiveness of ICoFR".

To help the SEC address the immediate "pain point" associated with a lack of practical and cost effective guidance for management *and*, perhaps even more importantly, to move more aggressively on the path to global harmonization on reporting on ICoFR, the IMA is taking the following steps:

1. Expose this discussion draft on assessing ICoFR to knowledgeable experts around the world. The IMA believe this draft represents a solid starting point for focused and timely discussion and debate on this important topic.
2. Actively engage a broader community in the debate including organizations specializing in quality management, IT security, fraud prevention/detection, risk management, business ethics, and others with a direct vested interest in the sufficiency and appropriateness of "how to" assessment guidance for management.
3. Seek input on this discussion draft from the members of accounting and auditing organizations around the world.

Taken together, these steps should:

1. Produce practical, top-down/risk-based, scalable, and cost-effective risk and control assessment guidance for management with the flexibility to use, and bridge to, the predominant controls framework.
2. Produce an approach that better integrates with the many advances in the risk and quality management fields that have occurred over the past 25 years.
3. Accelerate progress towards the longer-term goal of achieving global harmonization of risk and control assessment frameworks (i.e. new GENERALLY ACCEPTED RISK AND CONTROL ASSESSMENT PRINCIPLES –"GARCAP") to assess and report on ICoFR.

ACKNOWLEDGEMENTS

Principle Author: Tim Leech FCA·CIA·IT, CFE, CCSA, MBA (majors in Accounting and Human Resources)

Tim's experience and credentials relevant to this draft discussion paper include:

- public accounting and auditing training and experience with Coopers & Lybrand Toronto
- internal audit experience with Westinghouse and Gulf Canada
- controllership experience with Gulf Canada Resources
- established a new practice area for The Coopers & Lybrand Consulting Group in 1987 called Risk and Control Management Services focused on forensic accounting, CRSA, business ethics, fraud vulnerability assessments and internal audit reengineering
- extensive forensic accounting experience including expert witness testimony with Coopers & Lybrand, Gulf Canada, NCM Control & Security Management Services, and Leech & Associates
- author of CARD®*map* software, the world's first integrated CRSA/Internal Audit/ERM software
- Chief Methodology Officer and Principal Consultant, Paisley Consulting, a global leader in governance, risk and compliance software
- author of scores of articles, webcasts and e-learning modules on CRSA, ethics, SOX, internal audit and global trends in ERM published in IIA, IMA, CGA, CPA journals and acknowledged global speaker on related topics
- global consultant and trainer in the areas of CRSA, internal audit, SOX, Basel II, and ERM including assignments for major Fortune 500 organizations in North and South America, U.K, Europe, Asia, Africa and the Middle East
- co-author of the Financial Executives Research Foundation study *Control Deficiency Reporting: Review and Analysis of Filings During 2004*
- co-author of *Sarbanes-Oxley: A Practical Guide to Implementation Challenges and Global Response* published by Risk Books
- author of the IMA SOXERM e-learning modules on Sarbanes-Oxley legislation, regulation and implementation methods and challenges
- recognized by the Ontario Institute of Chartered Accountants as a Fellow of the Institute of Chartered Accountants for distinguished service to the profession and the Association Certified Fraud Examiners for meritorious service in the detection and deterrence of fraud; and
- primary author of the September 2006 IMA discussion paper *A Global Perspective on Assessing Internal Control Over Financial Reporting*.

Contributing Author: Jeffrey C. Thomson M.S.

Jeff Thomson has significant practitioner and academic experience in management accounting and related fields.

His business experience primarily consists of a 23-year stint at AT&T, where he served in many "front line" decision support finance roles including: competitive analysis; CFO for AT&T's first set of integrated offers to large business customers; conceiving and helping launch new products and markets; and, enterprise risk management applied to business turnaround situations. In Thomson's last position at AT&T he was CFO of AT&T's multi-billion dollar sales unit, which measured customer segment profitability. He was responsible for many "firsts" while at AT&T, including the first major telecom to successfully implement Activity-Based Costing.

Thomson is also a published author and global speaker in the areas of strategic planning, EVA (economic value added), ABC and evolving strategic costing approaches, performance management, competitive analysis, statistical process quality control and enterprise risk management. He has been an adjunct professor of business mathematics for over 25 years.

Thomson joined the Institute of Management Accountants as Vice President of Research and in less than one year put IMA "back on the map" with one of the most comprehensive and relevant research programs in the profession. This document is an example of this drive. Thomson has conducted scores of media interviews and webinars in addition to being a primary author on many articles and a contributing author to several books, research studies and articles.

Thomson holds an M.S. in Mathematics and Statistics, with executive education from Wharton and Columbia Business Schools in finance, accounting and leadership.

Contributing Organizations and Individuals:

A wide range of organizations and experts in areas relevant to this paper have been invited to provide constructive comments and feedback. All Participating Organizations and Individuals that submit comments will be recognized in the final version of this paper.

1. SCOPE AND GENERAL

1.1 Scope and Application

This guidance provides a broad principles-based assessment approach organizations can use to guide their efforts when they are required by law and/or regulation, or voluntarily elect, to report to relevant stakeholders on the reliability and effectiveness of internal controls over financial reporting. It is specifically designed to recognize the role that regulators play prescribing ICoFR assessment criteria and, most importantly, explicitly or implicitly deciding on "fault tolerance" or "residual risk tolerance" criteria. The level of granularity regulators impose on public companies, both big and small, as mandatory requirements has a direct impact on the cost of compliance. Examples of regulatory requirements in this area include the type of formal certifications on internal control effectiveness currently required from SEC registrants pursuant to the Sarbanes-Oxley Act of 2002, particularly the SEC/PCAOB definitions of what must be assessed and how, in Canada, the control certifications that will soon be required from CEOs and CFOs in Canada pursuant to Multilateral Instrument 52-109; and in the U.S. federal public sector, declarations from senior management pursuant to OMB Circular A-123. Similar rules in other countries are evolving.

NOTE: Guidance and suggestions in this document must always be subordinated to applicable laws and regulations on how to complete an assessment of ICoFR where those laws and regulations differ and/or are more prescriptive than the broad principles-based assessment approach advanced in this document.

It is expected that, over time, a growing number of jurisdictions around the world will enact some form of directionally consistent laws and regulation related to mandatory management reporting on ICoFR as the value of this new information from management becomes better understood and more broadly accepted and acknowledged.

In addition to national securities regulatory bodies and standards-setters, other groups that should find this guidance and information relevant and useful include 1) Management – management has primary responsibility for ICoFR and should find this discussion entirely relevant, 2) internal auditors that assist management with their efforts in this area, 3) boards of directors that must oversee the adequacy of the processes established by management to provide assurance external financial disclosures are reliable, 4) professional services firms that provide advice and support services, 5) external audit oversight agencies and associations, and 6) investors, credit providers and rating agencies, public sector constituents, and others that want to better understand the purpose, significance and limitations of this new information on ICoFR that is just starting to be provided in a significant way by management. Input and comment will be sought on this discussion paper from all these participants.

1.2 Objectives

In addition to the overarching objective of providing broad principles-based guidance on how to approach the task of assessing and reporting on ICoFR, the goal is to offer an assessment framework for ICoFR that enables organizations to realize full value and maximum possible return on investment from their compliance programs by offering the following attributes:

- **Provides an assessment framework that is "scalable**". We define scalable to mean a risk and control assessment framework that can be used by any size of organization that must by law, or voluntarily elects to, provide formal management assurances on ICoFR. The focus on scalability addresses concerns raised in March-April 2006 timeframe by the SEC Advisory Committee on Smaller Public Companies.
- **Provides a framework that directly focuses on ways to contain ICoFR assessment costs while still providing a high level of assurance that financial disclosures are reliable.** The assessment approach being proposed in this paper is based on risk rating a universe of ICoFR "assurance contexts" and identification of symptoms or key risk indicators in that assurance universe that suggest heightened risk of unreliable financial disclosures. When such symptoms are present, the amount of assessment and testing recommended should be proportionately increased, much the same as the approach used by medical doctors when assessing the health of a patient. We do not believe society can bear the cost of extensive assessment and testing on the entire potential assurance universe that supports a company's financial statements when there are few, if any, performance and/or risk indicators present that indicate a problem might exists.
- Provides input to the Securities Exchange Commission in response to the July 11, 2006 ***Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting*** to assist the Commission in their deliberations.
- **Provides an interpretation of the term "top-down/risk-based"** assessment that is consistent with global risk and quality management standards and tangible guidance how to approach assessments of ICoFR from that vantage point.
- **Provides a framework that helps management complete control assessments** 1) at the entity level over the financial statement preparation and disclosure process, 2) on the reliability of an organization's anti-fraud controls as they relate to external financial disclosures, 3) on the reliability of IT general controls as they relate to external financial disclosures, 4) on line item disclosures in the financial statements and individual general ledger accounts that comprise them 5) on note disclosures in the financial statements.
- **Provides a framework that**, in addition to its applicability to ICoFR, **can also be used to "risk rate" and assess risk and control on any dimension of enterprise risk and operational risk management** including product quality, customer service, continuity of operations, IT security, physical security, terrorist vulnerability, cost minimization, general compliance and other issues.

While we recognize these are very ambitious goals we hope that, at a minimum, the proposals in this document spark valuable global research, debate and discussions on these subjects – desperately needed activities that will advance the world's knowledge of what it is required to produce consistently reliable financial disclosures (account balances and notes disclosures) at a reasonable cost to investors and society as a whole.

1.3 Reference Documents

1. Internal Control – Integrated Framework 1992/94
   Committee of Sponsoring Organizations of the Treadway Commission (COSO)
2. Guidance on Control, November 1995
   The Canadian Institute of Chartered Accountants
3. Guidance on Assessing Control, April 1999
   The Canadian Institute of Chartered Accountants

4. The Turnbull guidance as an evaluation framework for the purposes of Section 404(a) of the Sarbanes-Oxley Act, 16 December 2004, Financial Reporting Council
5. Internal Control Revised Guidance for Directors on the Combined Code, October 2005, Financial Reporting Council
6. Enterprise Risk Management – Integrated Framework September 2004, Committee of Sponsoring Organizations (COSO)
7. Australian/New Zealand Standard: Risk Management Standards Australia, Standards New Zealand AS/NZ 4360:2004
8. CobiT 4.0, Control Objectives, Management Guidelines, Maturity Models, 2005 IT Governance Institute
9. Aligning CobiT ®, ITIL® and ISO 17799 for Business Benefit, 2005, IT Governance Institute, Office of Government Commerce, The IT Service Management Forum
10. IT Control Objectives for Sarbanes-Oxley, 2nd Edition Exposure – 30 April 2006, IT Governance Institute
11. Information Technology – Code of Practice for Information Security Management, ISO 17799, International Organization for Standardization
12. Implementing the Professional Practices Framework, Christy Chapman, Urton Anderson, 2002, The Institute of Internal Auditors
13. Management Antifraud Programs and Controls: Guidance to Help Prevent and Detect Fraud, No date indicated, issued by AICPA, FEI, ISACA, IIA, IMA, SHRM
14. Internal Control Over Financial Reporting – Guidance for Smaller Companies, July 2006, Committee of Sponsoring Organizations of the Treadway Commission, PricewaterhouseCoopers LLP, Author
15. Final Report of the Advisory Committee on Smaller Public Companies to the United States Securities and Exchange Commission, April 23, 2006, SEC Advisory Committee on Smaller Public Companies.
16. Sarbanes-Oxley: A Practical Guide to Implementation Challenges and Global Response, 2005, Chan, Gupta, Leech. Risk Books.
17. IMA Research Study "COSO 1992 Control Framework and Management Reporting over Financial Reporting: Survey and Analysis of Implementation Practices", by Parveen P. Gupta, LLB, PhD, September 2006.
18. Risk Management and Internal Control in the EU – Discussion Paper, Fédération des Experts Comptables Européens March 2005.
19. Analysis of Responses to FEE Discussion Paper on Risk Management and Internal Control in the EU: A Comment Paper, Fédération des Experts Comptables Européens, May 2006
20. Internal Controls – A Review of Current Developments, International Federation of Accountants Information Paper, August 2006.
21. Control Deficiency Reporting: Review and Analysis of Filings During 2004, Parveen Gupta, Tim Leech, Financial Executives Research Foundation, 2005
22. Final Report of the Advisory Committee on Smaller Public Companies to the United States Securities and Exchange Commission, April 23, 2006.
23. ISO Guide 73 Risk Management – Vocabulary – Guidelines for Use in Standards, International Organization for Standardization, First Edition 2002.

24. Control Deficiencies Trend Alert: Control Deficiencies – Finding Financial Impurities: Analysis of the 2004 and Early 2005 Deficiency Disclosures, Glass Lewis & Co, Townsend and Grothe, June 24, 2005.

25. Guidelines for Managing Risk in the Australian Public Service, a joint publication of the Management Advisory Board and its Management Improvement Advisory Committee, October 1996.

26. Internal Control: Analysis of Joint Study on Estimating the Costs and Benefits of Rendering Opinions on Internal Control Over Financial Reporting in the Federal Environment, United States Government Accountability Office, September 6, 2006.

2. ICoFR Overview

2.1 Background

The primary goal of regulatory interventions like the Sarbanes-Oxley Act of 2002 in the U.S., particularly Sections 302 and 404, is simple – reasonably reliable public company financial statements. The term "reasonably" is subject to wide interpretation around the world. What is certain is that investors, banks, credit rating agencies, regulators, employees and others rely, to varying degrees, on the information contained in financial statements for a range of important purposes and decisions. It is increasingly accepted that to accomplish the goal of producing reasonably reliable financial statements management must design and maintain "effective" internal controls over financial reporting ("ICoFR"). By extension, to provide comfort to regulators and others that this is being done consistently management is now being asked, at least in some countries, to prove that they are periodically and formally assessing and reporting on ICoFR and have remedied situations identified that have the potential to lead to material errors in the financial statements. The term "effective control" like the term "reasonably reliable" is also subject to wide interpretation around the world.

The goal is certainly simple. In practice, it is a very difficult task complicated by a number of factors, most importantly the lack of general agreement on how to approach the task of assessing and reporting on ICoFR, as well as pronounced differences in the attitude of regulator's and auditor oversight bodies around the world to the role of external auditors "reworking" financial statements prepared by management prior to their release.

It is important to note that the terms "effective", "adequate" and "reasonably reliable" internal control can be defined inversely as:

> ***A combination of internal controls that produce a financial statement disclosure error pattern over some period of time that is viewed by relevant stakeholders, including securities regulators for public companies, as tolerable or acceptable.***

Whether the existence and rate of errors in the accounts and note disclosures produced by management should be evaluated before, or after, the external audit of the financial statements is complete, and the extent and nature of involvement of the external auditor assisting management with the preparation of the financial statements and notes and correction of errors and omissions are key questions that are just starting to be addressed by regulators, particularly in the case of smaller public companies that lack sophisticated specialist personnel and systems.

In the U.S., the SEC and PCAOB have, at least to date, taken the position that the adequacy of ICoFR should be assessed and publicly reported on before considering any corrections that occur as a result of the work of external auditors. Historically, investors and other users of financial statements have not been told much, if anything, about the frequency and magnitude of material errors in the accounts discovered by the external auditors that were corrected by management prior to the filings made with securities regulators.

To date in the U.S. the specifics of how management should complete their assessment of ICoFR for SOX Sections 302 and 404 has been primarily guided by the approach mandated by the PCAOB for external auditors in Auditing Standard No. 2. An IMA SOX research study

entitled "COSO 1992 Control Framework and Management Reporting on Internal Control over Financial Reporting: Survey and Analysis of Implementation Practices" confirms this assertion. In the study, 62% of the nearly 400 seasoned respondents indicated that they actually used AS2 to guide their assessments, while 38% claimed they used COSO 1992. As a result of the SEC May 17, 2006 announcement that they will be issuing guidance for management on assessing ICoFR, and their subsequent issuance of a Concept Release on management's reports on ICoFR requesting feedback, it is likely that there will be some reforms over the next year in the U.S. to address widespread concerns raised by the business community.

As noted earlier in this paper, the SEC has stipulated management should use a control assessment framework that meets the SEC's "suitability" criteria. Their decision to issue their own control assessment guidance for management suggests that the SEC has concluded that existing control assessment guidance for management, including the new COSO SPC guidance, is not adequate on a standalone basis. The September 2006 IMA SOX research study indicates fairly conclusively that companies have experienced difficulty using the 1992 COSO Internal Control Integrated Framework as primary SOX assessment guidance for management.

IMA Research Study: Is it Possible to arrive at a Reliable Pass/Fail Conclusion on ICoFR Using COSO 1992? (Table 23)

Response Scale	# of Respondents (N = 327)	% of the Total Sample	Small Companies (N = 62)	Medium to Large Companies (N =265)
1. No Extent	8	2.4%	0%	3%
2. Some Extent	163	49.8%	58.1%	47.9%
3. Moderate Extent	59	18%	16.1%	18.5%
4. Large Extent	72	22%	16.1%	23.4%
5. Uncertain	25	7.6%	9.7%	7.2%

The most recent guidance issued by COSO for smaller public companies has made a number of important strides to try and address deficiencies and concerns in the management assessment guidance available for companies of all size. Work is ongoing in this area.

In Canada, pursuant to Multilateral Instrument 52-109, the regulators, at least to date, have left the decision of how management should complete the required assessment of controls largely to their own discretion. Canada originally announced that it would follow the U.S. approach to management reporting on ICoFR with few, if any, variations on the U.S. SOX rules. A decision to cancel the Canadian equivalent of SOX Section 404(b) was announced by the Canadian Securities Administrators on March 10, 2006 in CSA Notice 52-313. Whether Canada will issue its own guidance for management on how to assess ICoFR is uncertain at the current time. Auditing firms and consultants will likely use the U.S. rules related to ICoFR as primary approach guidance when working with Canadian listed firms. Cancellation of Multilateral Instrument 52-111 in Canada means external auditors of Canadian public companies will not be required to publicly report their views on the how well management has discharged their responsibility to report on the effectiveness of ICoFR, or their own opinion on the effectiveness or adequacy of ICoFR as is currently the case for SEC registrants.

Other countries including the U.K., Europe, Japan and others are at various stages contemplating whether to follow the path taken to date by the U.S., or employ some other strategy to increase stakeholder confidence that the financial statements of public

companies that come under their jurisdiction are reliable. At this point it appears the general international consensus is not to follow the lead of the U.S. in this area.

This discussion draft sets out a principles/risk-based approach on how the task of assessing and reporting on ICoFR could be approached to satisfy the goal of more reliable financial statements at an overall cost that is lower and produces greater business benefits than the current management assessment methods being employed to meet existing U.S. rules, particularly Auditing Standard No. 2 ("AS2") issued by the Public Company Accounting Oversight Board.

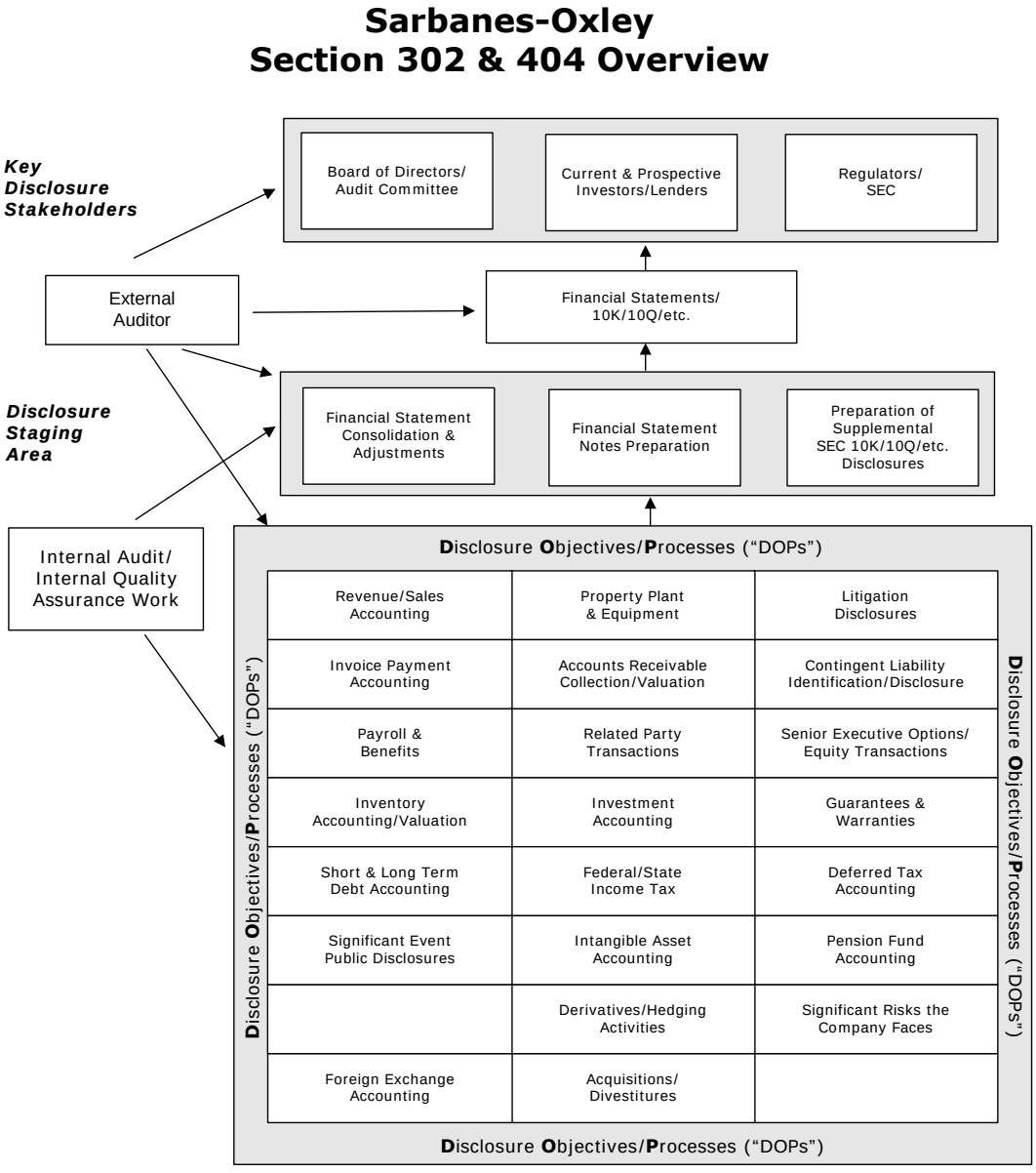
The key challenges in developing true top-down/risk-based guidance are 1) the willingness of regulators, external auditor oversight groups, and management that have already made major investments in other assessment methods, particularly more granular and costly bottom-up control assessment approaches fostered by AS2 to embrace true top-down/risk-based assessment methods (i.e. the "sunk-cost" challenge); 2) the desire of at least some percentage of regulated companies, their advisors, and the external audit profession for assessment guidance that provides detailed "how-to" information, including preset checklists that can be completed and filed by management and auditors as evidence of compliance and, perhaps most importantly; 3) the challenge of addressing how to help companies that have already made major investments and done massive amounts of work but want a more efficient and effective process going forward transition from "bottom-up", control centric assessment approaches to one that it is truly "top-down/risk-based" (i.e. the "bridging" challenge).

2.2 The Primary Goal

Visualizing the Goals of ICoFR

The fundamentals of ICoFR can be explained using the diagram below. The primary goal of an ICoFR system from a regulatory perspective is aptly summarized in the purpose statement of The Sarbanes-Oxley Act of 2002:

> ***To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws, and for other purposes.***



For the management and boards of public companies, private companies, public sector organizations, and not-for-profits the primary goal can be expressed simply as:

Produce reliable auditor certified external financial disclosures.

For key stakeholders to evaluate and make decisions related to any organization, large or small, be it a bank, insurance company, oil company, manufacturer, retailer, health care provider, private or public sector entity, they need reliable information on the history, current financial status and future prospects of the company. Key Disclosure Stakeholders are depicted in the top portion of the overview.

Primary data sets used by the various disclosure stakeholders are monthly, quarterly, and annual financial statements, notes to the financial statements, and important supplemental disclosures. These data sets can be assembled, consolidated and reported at multiple levels of an organization (i.e. they may be developed in a subsidiary and then roll up to a parent company for consolidation). These activities are depicted simply in the ICoFR Overview as steps that occur in the “Disclosure Staging Area”. Staging Area activities have been subdivided in to three core activities:

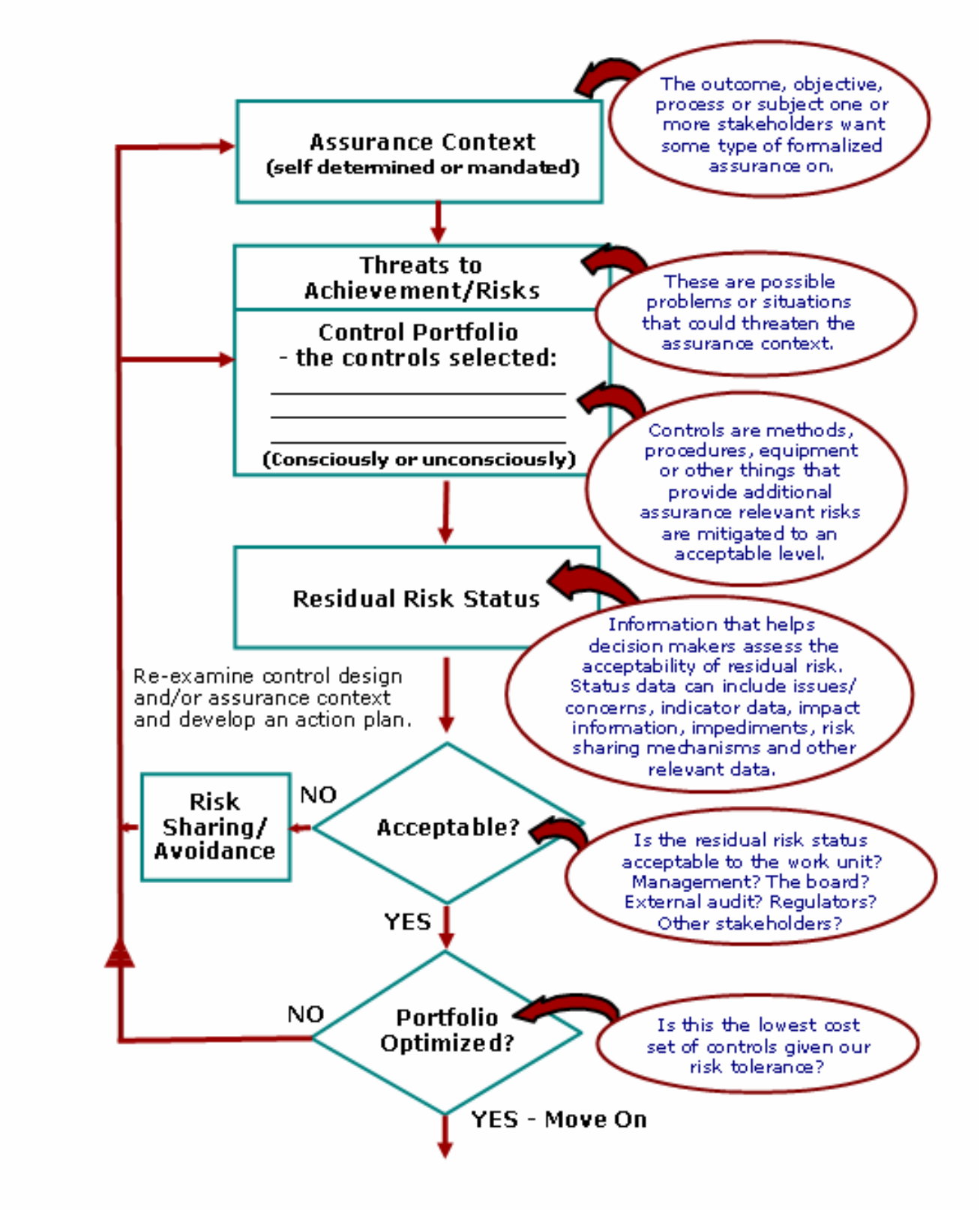
Financial Statement Consolidation and Adjustments
Financial Statement Notes Preparation
Preparation of Supplemental Disclosures

The data necessary to assemble the disclosures comes from a wide range of sources. Illustrative information sources are depicted in the overview as a universe of “Disclosure Objectives/Processes” ("DOPs"). Each DOP has an associated end result objective of timely and reliable disclosure of some sub-set of the company's disclosure package; and a process or system, including internal controls that support it and manage risks that would cause it to be unreliable. The DOPs depicted in this overview are not exhaustive and will vary depending on the size, complexity and business sector of the organization. Some of the DOPs are highly automated and flow information to the Disclosure Staging Area via sophisticated computer systems. Others are partially automated and may include the use of tools like spreadsheets. Some are done manually and involve significant levels of estimation and judgment. The DOPs must deliver generally reliable and complete information to the Disclosure Staging Area for the final consolidated package to be reliable. In cases where they don’t, the onus is on the controls in the Disclosure Staging Area, including the quality assurance work done by senior management and external auditors, to detect errors. Some of the DOPs are particularly significant and capable of creating material and dangerous disclosure problems while others are less critical. (See Section 3.3 for a suggested risk rating system.)

A wide variety of risks threaten the goal of reliable financial disclosures at all stages of the production process much the same way that the final quality of a product produced in a factory can be threatened at all stages of the manufacturing process, starting with product design decisions, design of production process and the ordering of raw materials.

It is important to note that many of the biggest corporate frauds in history have occurred in the Disclosure Staging Area at a level well above the more micro DOP control processes. Highly visible examples include Enron, WorldCom, HealthSouth, Parmalat, and many others.

2.3 Core Components of a Risk-Based Approach



The core elements of the risk-based ICoFR assessment process being proposed are depicted above. The primary goal is the creation and maintenance of a continuous process that works towards the goal of key stakeholders understanding and agreeing on the acceptability of the current "residual risk status". Although it is a somewhat subtle difference, the emphasis in this approach is on seeking understanding and consensus agreement between management and external auditors on what the current residual risk status is currently, not subjective views of management and external auditors of what constitutes "effective" or "adequate" ICoFR in their minds. This process is NOT intended to be rigid and prescriptive, rather, it is intended to supplement management and external auditor's intuition and judgment with tangible facts and data.

The recommended emphasis on seeking consensus understanding between management and external auditors on the current residual risk status flowing from the current controls in place conflicts with current SEC rules that require both auditors and management make specific public representations whether each party, independent of the other, believes that ICoFR is, or is not, "effective". **We believe seeking consensus on whether control is, or is not, "effective" creates a number of serious problems including unproductive debate, high costs, and serious litigation risk to management and auditors that could be reduced if the focus was redirected to agreeing that management and external audit both have a reasonable understanding of the residual risks** that exist that could potentially impact on the reliability of financial statement disclosures. External auditors around the world including those in the U.S. for public companies, private companies and the public sector, are still regularly certifying financial statements as reliable in organizations that have internal control systems that have low reliability and have received limited formal assessment by management or the external auditors, including organizations that have required on a regular basis material adjustments to the financial statements prior to auditor certification. We provide further commentary on this issue in Section 4 – Global Regulatory Considerations.

Identifying the Assurance Context

The risk-based approach proposed in this paper starts with an "Assurance Context". The word "context" is drawn from the widely acclaimed and recognized Australia/New Zealand Risk Management Standard 4360. When combined with the word "assurance" this term describes the outcome, objective, process or subject that one or more relevant stakeholders want some type of formalized and positive assurance on. (assurance is defined as "a positive declaration intended to give confidence") For purposes of this discussion paper**, it is important to note that the macro level assurance context focused on in this paper, reliable auditor certified external financial disclosures, is only one relatively narrow component of what it takes to achieve long-term business success. The approach described in this paper has been successfully applied to all types of assurance contexts including those related to product quality, customer service, cost minimization, general compliance, safety, cost control, fraud prevention, national security, revenue maximization and others.**

The macro level assurance context of **reliable auditor certified external financial disclosures** can then be further delineated in to assurance context sub-components including the following:

- External financial disclosures are in accordance with applicable GAAP and regulation.
- Specific account balances that form the elements of the line items in financial statements are reliable and in accordance with GAAP and applicable regulation.

- Financial statement note disclosures are reliable and in accordance with GAAP and applicable regulation.

- Business processes that support accounts and note disclosures in financial statements are reliable.

Examples of assurance context sub-elements related to IT security that directly impact on the broad objectives above include:

- Software programs that impact on the company's financial statements are reliable.

- Data stored in IT systems that impacts on the accounts and note disclosures is secure.

These IT assurance contexts can be further delineated to all sub-elements that support these broad aims.

How to tackle an assessment of these assurance context statements using a risk-based approach is described in more detail in this discussion paper.

Identifying Risks or Threats to Achievement

The next core element is the activity of identifying and assessment of risks or threats to the assurance context. These can be defined as possible problems or situations that could result in the non-achievement of the assurance context. AS/NZ 4360 defines the word "risk" even more broadly as the chance of something happening that could have an impact on objectives. In holistic risk management "risk" can have positive and negative impact. For purposes of ICoFR for regulatory purposes, the emphasis is on identifying and assessing the likelihood and consequences of situations or events that have the potential to cause a material error in the financial statement accounts and notes disclosures only (i.e. "down-side" risks as opposed to "upside" risks) Production of financial statements that are more reliable than is required by external auditors and applicable laws does not generally represent an area of concern for regulators. However, it is important to note that the idea of excessively accurate financial statements can be a valid consideration for management if the additional unnecessary accuracy/reliability comes at a high direct or indirect cost to the organization.

RECOMMENDATION TO U.S. REGULATORS: The current U.S. regulations place considerable emphasis on identification of account and note "assertions. The term "assertions" is not part of generally accepted generic risk assessment methodologies or taxonomy. Account assertions can be thought of as either sub-elements or specific attributes of the assurance context, or stated negatively as risks. An example would be inventory balances disclosed in financial statements. A sub-element of whether this public disclosure is actually reliable is that it exists. To be a reliable disclosure it must exist. A risk to the reliability of the inventory account balance is that some or all of it doesn't exist. **We are recommending an assessment approach that does not use the term "assertion" as part of the core methodology. Existing guidance and assertion documentation that has been produced can be easily rewritten as risks to the assurance contexts being assessed.** The reason for this recommendation is that we believe the assessment approach used by management for ICoFR should be capable of being used to assess any type of assurance context including product quality, customer service, safety, security or any other relevant attribute versus an assessment approach that

can only be used to assess ICoFR. **We believe fostering the adoption of a generic risk and control assessment approach that is useable for the full range of assurance contexts in a company produces maximum business benefits as opposed to assessment approach that is only relevant to ICoFR.** In short, achieving broader acceptance by work units and demonstrating improved "ROI" for upper management are possible with a more inclusive definition of risk and controls management that can be extended beyond the financial compliance domain.

Identifying the Current Control Portfolio

The next step in the assessment process is identification of the current "control portfolio". The control portfolio represents the collection of controls and/or strategies that an organization has chosen, consciously or unconsciously, to mitigate relevant risks to the specific assurance context being evaluated. The term "portfolio" is used to connote the concept that this is a collection of controls that has been assembled that is more or less risky similar to a portfolio of investments.

NOTE: In pure forms of risk management like the approach espoused in AS/NZ Risk Management Standard 4360, the accepted terminology is to "treat" the risks. "Risk treatment" is defined as the "process of selection and implementation of measures to modify risks". Using internal controls to treat or mitigate the likelihood and/or consequences of risks is only of the four standard risk management options available. The standard risk management options include **avoid** the risk by exiting the business, line of business, area causing the risk, or other techniques; (an example in ICoFR would be to not enter in to leases that meet the accounting criteria of being "capital leases" to avoid the increased risk of accounting error or avoid countries or lines of business prone to major fraud); **share** the risk using vehicles like insurance, outsourcing, and/or contractual mechanisms; (an example in ICoFR could be the outsourcing of all pension fund accounting responsibilities and creation of indemnity clauses if the accounting done by the outsourced provider was proven to be inaccurate); **mitigate** the likelihood and/or consequences of relevant risks using internal controls; and lastly, **accept** the risk. For ICoFR, accepting risks means accepting some chance or level of chance that the company will release materially unreliable financial statements. The emphasis of external regulators to date, particularly in the U.S., has focused heavily on the option of mitigating risks using internal controls and requiring binary conclusions on control effectiveness, more specifically, focusing on requiring management and auditors report on whether the current controls are, or are not, "effective". The reality is that "effective" controls can be defined as the combination of controls that reduce risk to a residual level acceptable to one or more of the stakeholders. **This draft is proposing an approach that focuses on identifying and seeking consensus agreement on the acceptability of the current residual risk status, the risk that remains after all "risk treatment" measures have been considered.** To acknowledge the current U.S. regulatory emphasis on the single dimension of using internal controls to mitigate risks versus identifying situations where risk sharing or avoidance is available, more time and attention has been is dedicated to the option of mitigating risks using internal controls.

Control frameworks such as COSO 1992, CoCo, Cadbury, COSO Guidance for Smaller Public Companies 2006, COSO ERM, and CARD®*model,* a COSO linked and derived framework interpretation shown in the Attachments section of this paper provide different perspectives on the elements or criteria that make up an organization's integrated control or "risk treatment" macro/micro framework.

Each of these "control frameworks" organizes the total universe of possible controls somewhat differently, and each one puts more, or less, emphasis on different sub-

components of internal control. They describe the full range of control "elements" that are available to provide assurance on various assurance contexts. (NOTE: It is important to emphasize that, to date, none of the control frameworks listed above have been empirically tested to validate the premise that organizations that have been assessed by auditors as fully conforming to the stated control attributes or principles actually produce more reliable financial disclosures than those that don't.)

COSO 1992, the dominant U.S. framework, employs five broad control category descriptors to discuss the core elements of an integrated internal control framework - Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring.

In 1994 the **Cadbury Report** in the U.K. generally endorsed the 5 COSO 1992 primary control categories but wanted more emphasis on the processes management employs to determine and communicate what they termed control objectives. Cadbury amplified the COSO 92 Risk Assessment category and renamed it "Identification and evaluation of risks and control objectives" and extended the COSO 92 "Monitoring" category to "Monitoring and Corrective Action". COSO 1992 explicitly stated on page 21 of the May 1994 Executive Summary that "Corrective actions" is a management activity that is not an element of internal control. The authors of the Cadbury/Turnbull framework did not agree with that conclusion. The U.K. Turnbull guidance has recently moved even closer to the U.S. based COSO 92 categories as a result of pressure to use the COSO 1992 framework, largely from the auditing and consulting community. The U.K. framework is included as Attachment 7.

The **Canadian Criteria of Control framework** included as Attachment 6, generally known as CoCo, was originally released in 1995. The authors of CoCo elected to use a radically different way of grouping and defining the elements of control. CoCo organizes controls under four somewhat more people focused categories – Purpose, Commitment, Capability and Monitoring and Learning. Under these four primary CoCo control categories there are a total of 20 "control criteria" or control category sub-elements. The Canadian guidance includes details on how the 1995 CoCo guidance "builds on the concepts in the COSO document" On page 27 a section titled "COMPARISON TO COSO" outlines the key differences between COSO 1992 and CoCo. One of the most noteworthy differences is described on page 29 in the CoCo guidance:

CoCo includes the following definition of effective control: Control is what makes an organization reliable in achieving its objectives. Control is effective to the extent it provides reasonable assurance the organization will achieve its objectives. Or, stated another way, control is effective to the extent that the remaining risks of the organization failing to meet its objectives are deemed acceptable.

A **COSO-linked framework, CARD®*model,*** shown as Attachment 8 uses a control categorization system that represents a blending of ideas from COSO, CoCo and the U.K. guidance. The primary control categories or groupings are Purpose: Definition and Communication, Commitment, Planning & Risk Assessment, Capability/Continuous Learning, Direct Controls, Indicator/Measurement Controls, Employee Well-Being and Morale and Process Oversight. Each category represents the controls an organization has in place to address 8 core control criteria, described in page 68. The key differentiators promoted by this assessment system is an emphasis on measurement and commitment controls and seeking identification and consensus agreement on the acceptability of the current residual risk status related to an organization's assurance contexts and objectives. All control

elements in COSO 1992, COSO ERM, COSO SPC, CoCo and Cadbury are represented in this COSO linked framework.

The **COSO Enterprise Risk Management (ERM) - Integrated Framework** issued in September of 2004 merges the COSO 1992 framework with the type of thinking in the dominant recognized risk management frameworks, in particular the Australia/New Zealand Risk Management Standard 4360 originally issued in the mid 1990s and ISO guidance on risk management. U.S. regulators, the COSO Committee, and the global external auditing profession have not, at least to date, encouraged the use of the 2004 COSO ERM framework, or any of the widely accepted risk management standards such as AS/NZ 4360, for purposes of reporting on ICoFR for SOX, although there have been repeated calls for ICoFR assessments to be "risk-based".

The **COSO Smaller Public Company** ("COSO SPC") guidance released in final in July 2006 utilizes the same 5 control categories contained in COSO 1992 but articulates 20 "control principles", much like the 20 "control criteria" articulated in the 1995 CoCo framework in Canada. COSO SPC emphasizes that management specifying financial reporting objectives is a key element of assessing ICoFR. This differs somewhat from the original COSO 1992 framework that explicitly stated that "Entity-level objective setting- mission, value statements" and "Activity-level objective setting" are not part of a company's internal control system (page 21 of the May 1994 COSO Executive Summary). The focus of the new COSO SPC guidance is on describing an approach to assessing ICoFR specifically for purposes of helping smaller public companies comply with the SOX regulations in force when this guidance was developed (although the guidance also indicates that the principles and sub-attributes mapping to the 5 core control categories can be applied to any size company).

Section 3.5 of this draft provides more guidance on how the available control frameworks including COSO 1992, CoCo, COSO SPC, COBIT, and CARD®*model*, a COSO linked model can be used to assist organizations with the task of identifying and assessing the adequacy of their current "control portfolios" for the ICoFR assurance contexts.

Identifying the Current Residual Risk Status

Once the controls in place to mitigate risks to the assurance context have been identified, the net result of those choices at any point in time in the risk-based methodology proposed in this discussion paper is called the current **RESIDUAL RISK STATUS**. A composite picture of the current residual risk status is made up of a range of relevant information that helps decision makers assess the overall acceptability of residual risk related to the assurance context being evaluated. This element of our recommended approaches differs from other more traditional assessment approaches that focus on documenting control processes, testing the execution of prescribed controls, and identifying residual risk only as it relates to individual risks as opposed to the overall residual risk status related to a particular assurance context being assessed.

Key residual risk status sub-elements in this approach include **INDICATOR data**, data on how well the assurance context objectives are being achieved including errors detected and/or losses incurred (in quality terminology this is sometimes called process error rate and other information on performance); **CONCERNS**, representing risks that may not be mitigated in whole or in part by existing controls that have been identified to date, often called control deficiencies or issues for purposes of ICoFR; **IMPACT data**, data that helps decision makers understand the consequences of non-achievement of the specific assurance context(s) both financial and non-financial (an example for ICoFR would be debating the

impact of a misstatement between two expense line items with no impact on net profit – what are the potential impacts, if any); **IMPEDIMENTS**, representing situations or problems that exist that make it difficult or even impossible to treat the risk using controls only (an example in ICoFR might be legacy accounting systems developed over the past 20 years with minimal systems development and change controls); and **RISK SHARING STRATEGIES**, including details on how the risk has been shared with another party and any exceptions where the other party would not acknowledge responsibility.

Residual risk is defined by the dominant risk management standard, AS/NZ 4360 as the "risk remaining after implementation of risk treatment". Risk treatment, in addition to selecting internal controls to address the risks identified, can include things like insurance, transfer or sharing of responsibility for various risk elements via contract, avoidance of the risk and, perhaps most importantly, acceptance of certain risks and the consequences that flow from that acceptance by management and boards of directors. These risk management concepts are all relevant to ICoFR since organizations can outsource responsibility for elements of their processes that produce external financial disclosures, can elect to exit lines of business or geographical areas that could threaten the reliability of external financial disclosures, can take steps to buy insurance coverage that may reduce the consequences that can flow from unreliable financial disclosures, and, most importantly, can accept that the draft accounts turned over to external auditors may still contain some number of material errors, omissions, and misstatements that may, or may not, be corrected in the course of the external audit. In an ideal world the cost of a company's external audit would be directly linked to the amount of external audit inspection and rework required (a parallel in manufacturing is production processes that routinely produce products that contain some number of product flaws).

Assessing Acceptability of Residual Risk Status

Once risks, controls, and residual risk status related to the assurance context have been identified and documented the next core step is **making decisions on the acceptability of the current residual risk status.** This is the step where the board of directors, management, staff at all levels of any organization, external auditors, and regulators make decisions on whether they are comfortable with the risk that remains that the company might issue materially unreliable auditor certified financial statements. Some of the ICoFR assessment approaches that have been used to date focus heavily on whether control activities identified during process mapping exercises are being done with limited and sometimes no direct focus on evaluating whether the current control design is, in fact, resulting in a level of residual risk related to undetected material error that is acceptable to all key stakeholders.

The assessment of acceptability of residual risk is an area that national regulators around the world play a major and growing role. Historically regulators have shown fairly high tolerance, but not unlimited tolerance, to public companies issuing financial disclosures that are later found to contain major errors. At the current time, U.S. regulators would appear to be expressing the lowest tolerance level for public disclosure of materially wrong auditor certified financial statements. The tolerance of senior management and boards of directors in all types and size of organizations to the risk of issuing false or misleading financial statements varies widely, much the same as the tolerance of companies to selling products that contain some number of faults or defects varies widely. (Note: On a personal level the tolerance of individuals for their family's and their own personal safety and health is another example of how people approach the concept of residual risk acceptance in real life.)

In the U.S. the PCAOB in Auditing Standard No. 2 has articulated criteria to grade control deficiencies (or stated another way grade residual risk concerns) into three primary buckets - low level/low impact control concerns, significant control deficiencies, and material control weaknesses. Control deficiencies that are rated as significant deficiencies or material weaknesses must, by law for SEC registrants, be reported by management to the company's external auditors and audit committee. Registrants have been encouraged by the SEC to describe the specific risk(s) or account balances that are at risk because of the disclosed control deficiency but are not forced to currently by PCAOB AS2. The existence of even one material weakness requires that management publicly announce in SEC filings that their ICoFR is ineffective via SEC filings. The SEC and PCAOB have gone further and said that any time the company's external auditor finds a material error in the draft accounts provided by management the company must publicly report the situation as at least a significant control deficiency, and it should be viewed as a "strong indicator" of a material control weakness. This is a very marked change in regulatory tolerance for weak ICoFR and residual risk.

Few, if any, countries other than the U.S. have announced their own criteria or required that public companies use a standardized system to grade and report on deficiencies in ICoFR. Canada, the U.K. and the EU have all publicly stated that they disagree with the current rules in the U.S. requiring a company's external auditor to form their own opinion on control "effectiveness" and current U.S. rules requiring that management make representations on whether they do, or do not, have an "effective" system of ICoFR using the same criteria in-force in the U.S.

The acceptance of external auditors playing a key role identifying and assisting management with financial statement error corrections and adjustments is a situation that is still widely viewed around the world as not only common and generally acceptable, but a standard way of preparing external financial disclosures in organizations, both big and small, in the public and private sectors. This situation is particularly true in smaller public companies and some public sector organizations that lack the personnel and systems to prepare reliable GAAP compliant financial statements and rely heavily on their external auditor/accountants to identify major errors and help with "rework" of the accounts/notes prior to publication. The issue of whether ICoFR residual risk is assessed before, or after, external audit inspections (which are themselves a type of control) is one that is a key element of the current objections being raised by small cap companies in the U.S.

At least some countries around the world in addition to the U.S. are currently evaluating whether investors should be provided with information on the current state of ICoFR and, if so, what.

Assessing Control Design Optimization

The last step after assessing the acceptability of residual risk status is to assess whether the controls in place represent the lowest cost combination of controls that would still produce an acceptable residual risk status. Although regulators are not generally concerned whether management is completing this step, investors should be very interested that management is maintaining cost effective controls that consider the cost of the controls versus the benefits of the controls in place, including avoidance of the negative consequences that come from false or misleading financial statements. Pushing the delicate balance between control cost minimization and the reliability of financial statements can lead to situations where financial statements with material errors are discovered by external auditors and corrected or, sometimes, released to the investing public.

2.4 Quality Principles & ICoFR

Historically, the external audit profession and the regulatory bodies that oversee them in virtually all countries around the world have taken the position that auditors can independently assess the state of ICoFR in an organization at a high level and, based on that assessment, adjust their work plan in such a way that they are able to identify any material errors in the accounts and note disclosures prior to release of auditor certified financial statements. This has been generally true regardless of the effectiveness of the ICoFR framework maintained by the company. This was certainly true in the U.S. prior to SOX, and continues to be true in most countries around the world. In cases where the external auditor identifies material errors in the draft financial statements it is expected that the company will correct or, in quality management vernacular, "rework" the statements before the auditor signs-off on the financial statements. In many respects the external auditor plays a role akin to that of an old style quality control inspection department at the end of a production line in a factory. The skill and tools external auditors use to complete their "inspection" of the accounts and notes prepared by management are critical to their global success rate identifying all material faults or errors in the accounts of the organizations they audit.

Users of audited financial statements are generally not aware of the extent of rework that occurs between the production of draft financial statements by management and the final auditor-certified finished product or the failure rate of the company's external audit firm globally identifying material errors in client accounts. The U.S. SOX regulatory regime represents the first tangible evidence that at least one country has decided that this approach to financial statement reliability is not producing an acceptable level of financial disclosure quality. Alternatively, stated another way, U.S. regulators have decided that this "inspection focused/rework as required" approach to financial statement quality is one of the main reasons for the unacceptable number of auditor certified, materially wrong financial statements. (NOTE: the North American manufacturing sector arrived at a similar decision many years ago after it became clear that the Japanese approach to product quality was outperforming North American methods in terms of quality.)

The current SOX regulatory regime, specifically PCAOB Auditing Standard No. 2, states that identification by the external auditor of a material misstatement in financial statements in the current period that was not initially identified by the company's internal control over financial reporting "should be regarded as at least a significant deficiency and as a strong indicator that a material weakness in internal control over financial reporting exists". The existence of even one material weakness requires that management disclose that the entire system of ICoFR is ineffective. The same rule applies in the event that a restatement of previously issued financial statements to reflect the correction of a misstatement is required. (NOTE: These are situations where the company's external auditor also failed to detect the material error before release.) Users are currently not told whether material control weakness disclosures being made in the U.S. are the result of this rule, or the result of proactive ICoFR assessment by management. To date, no other country in the world other than the U.S. has mandated that a company's management must publicly disclose to investors the company has ineffective ICoFR in all instances material errors are detected by external auditors in the draft financial statements.

Studies conducted by the Financial Executives Research Foundation and Glass, Lewis & Co. on SOX control deficiency reporting suggest that a large percentage of public material weakness disclosures from U.S. listed companies to date have occurred as a direct result of the PCAOB rule that says material errors in the accounts detected by auditors after management has signed off must, in most cases, result in disclosure of a material weakness

in ICoFR by management. What this suggests to the authors of this paper is that the predictive ability of management to proactively assess and remedy deficiencies in company's ICoFR prior to the date of discovery of material errors in the financial statements by a company's external auditors is still at a developmental stage.

The IMA believes that the end goal of a robust and effective ICoFR assessment system should be that management identifies and reports on the existence and/or potential for material error in the financial statements to the audit committee and the company's external auditors before the organization's external auditor identifies the existence of material errors in the accounts during the course of their audit. The well-known adage "BUILD QUALITY IN NOT ON" applies. The key end goal should be reliable auditor certified financial statements. Auditors that are aware of specific residual risks in a company's ICoFR should be able to adjust their work plan to compensate for the ICoFR deficiencies or, in a worst-case scenario, deny an opinion on the reliability of the financial statements and/or resign from the client engagement. Fairly conclusive evidence suggests that reliable auditor certified financial statements is the central issue that investors and other key stakeholders are really concerned about. They have shown only limited interest to date in management and auditor reports on internal control effectiveness. In Europe, the conclusion of a major review undertaken by the Fédération des Experts Comptables Européens is that investors are not interested to any significant degree in information on ICoFR provided by management or auditors. The interest of investors in information on ICoFR from management when in the same report the auditors are certifying that the financial statements are reliable is an area that warrants more research.

This discussion draft proposes specific steps to accomplish the overarching goal of reliable auditor certified financial statements in the next sections.

3. RISK-BASED GUIDANCE FOR ICOFR

3.1 Determine Key Stakeholders

When trying to solve a perceived problem it is important to take the time to identify and prioritize the key stakeholders that have a direct and indirect stake in solving it. The focus of the authors of The Sarbanes-Oxley Act of 2002 was clearly on investor protection. The stated purpose of SOX is:

> ***To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to securities laws, and for other purposes.***

All security regulators around the world that want to ensure the fairness and attractiveness of their capital markets share this goal. To date, only a few securities regulators have decided, at least at this point in time, that the frequency and magnitude of unreliable external financial disclosures in their jurisdiction by public companies is a big enough problem to their economies to warrant a major regulatory intervention. Some regulators, including those in Canada, the EU, the U.K., Japan and other countries agree that unreliable financial statements is in fact a major problem that should be addressed, but haven't yet decided how to address the issue beyond careful monitoring of the U.S. "SOX experiment".

In addition to capital market investors, venture capitalists, banks and other lenders, credit rating agencies, employees, pensioners, suppliers, customers, and many others rely to varying degrees on information contained in external financial disclosures. In addition to these parties, the senior management team of all organizations should care whether their internal accounting processes are producing reliable information for investors externally, and for resource allocations and strategic decision-making internally.

3.2 Establish the Risk Management Context

3.2.1 General

Agreeing that public companies should publish "reliable" financial disclosures is relatively easy. Agreeing just how reliable/error free the disclosures need to be and, most importantly, the consequences if they are not reliable, is far from easy. The fact that management's motivation, remuneration, goals and aspirations can sometimes conflict with the needs of other stakeholders, at least in the short-term, further complicates the issue. **"Establishing the risk management context" simply defined means understanding the internal and external environment and the reasons why the primary overarching risk that auditor certified financial statements contain material errors should be mitigated.** Understanding the interface between management's perspectives and motivations and those of regulators and outsiders, particularly the tolerance of both groups to the existence and/or potential of undetected errors in public disclosures is particularly important. It also means seeking agreement on how reliable or, stated another way, how unreliable/inaccurate financial statements can be and still meet the needs of relevant stakeholders. This information has major cost implications.

3.2.2 Risk Criteria – Big Picture Corporate Level

A primary goal of securities regulators is that public companies produce timely and reliable financial disclosures. The term "risk criteria" is defined in AS/NZ 4360 and the ISO Guide 73 *Risk Management Vocabulary – Guidelines for use in Standards* as "the terms of reference by which the significance of risk is assessed". In this discussion draft the **key macro level risk** is that the financial statements are not reliable or, stated another way, **auditor certified financial statements contain undetected material errors in account balances and/or note disclosures.**

Much has already been written about the implications of false or misleading financial statements to efficient and fair capital markets. Much more empirical study is needed to better understand the tolerance and reactions of investors to companies that publish unreliable/false financial statements. Although it is a broad generalization, it is probably fair to say that preliminary evidence so far suggests that investors on a global level have not been demanding information from management on ICoFR or pressing regulators for additional reforms in this area. In fact a number of parties in countries including Canada, the U.K., and the EU have specifically stated that they believe the pendulum has swung too far in this area in the U.S. **The implicit assumption in the current U.S. rules is that the extra layer of costly regulatory compliance rules related to ICoFR will produce more reliable auditor certified financial statements and investors will accept the extra costs being incurred by U.S. listed companies because they will accept that financial statements published by U.S. listed companies are, on balance, more reliable than financial statements of companies listed in other countries that don't have the same ICoFR quality assurance system.** This is a huge and untested assumption at this point that has been rejected to date by regulators and auditor oversight bodies everywhere in the world except the U.S. It is important to note that the U.S. federal government has also, thus far, not accepted the benefits of ICoFR requirements in SOX Section 404(b) regarding auditor certification, at least not in their current form.

While the broad national social and economic implications of unreliable financial statements and the attractiveness of a country's securities markets are certainly very important elements of the ICoFR debate, there are a number of other more specific risk criteria that have the potential to directly impact on the decisions of management and boards of directors related to the way they view the risk of releasing auditor certified unreliable financial statements.

Important risk criteria at the big picture corporate level include the following:

1. **Implications to the company's credit rating**. All of the major credit rating agencies have published papers in more or less detail on their attitude to control weaknesses disclosed under the current U.S. SOX regime. What they have not stated is how they obtain similar information in countries that do not require management and/or auditors make specific representations on ICoFR effectiveness, disclose material weaknesses in ICoFR, or the amount of rework of the accounts generated by the external audit. It is clear that the credit rating agencies do consider the track record of companies that have had to issue restatements of their financial statements and the reasons why these situations have occurred. One credit rating company, Moody's, has gone so far as to categorize SOX material control weaknesses as "Category A" and "Category B" issues. When a Moody's Category A control weakness is disclosed they have stated they aren't particularly concerned because they believe that external auditors can effectively "audit around" the problem. However, when what Moody's calls a Category B control weaknesses is

disclosed they consider these situations to be serious because they "question the ability of the auditor to effectively "audit around" a Category B weakness".

2. **Implications to the company's reputation**. Companies are increasingly concerned whether the market views its financial disclosures with some significant level of distrust and/or disbelief. When this situation occurs it reflects badly on the issuing company's senior management and board, as well as the external auditor that certifies the company's financial statements.
3. **Implications to the company's cost of capital.** The trust and reliance lenders place in management and management representations, and the "risk premium" lenders assign to an organization is often linked to the company's track record of issuing reliable audited financial statements. There is preliminary evidence that at least some lenders are starting to take an interest in information on ICoFR, but it is also likely fair to say that lenders have not shown high levels of interest in the current state of a company's ICoFR. It is important to note however that the attitude of credit rating agencies does directly impact on the views and decisions of lenders and investors.
4. **Personal implications to senior executives and board members.** The U.S. has shown the most zeal so far in punishing executives that have knowingly and/or negligently allowed their companies to issue false or misleading financial statements. The evidence in the U.S. is seen in the jail sentences being handed down, corporate and personal fines being levied, the legal threat of requiring bonuses be forfeited, civil actions being launched, and more. The attitude of the boards of directors of U.S. listed companies towards unreliable financial statements has been variable. Regulators in countries other than the U.S. have, as a general statement, not shown the same level of focus in this area. It is important to note that at least some companies that have a track record of unreliable external disclosures are experiencing difficulty attracting high caliber senior executives and board members, particularly CFOs and audit committee members, and having to increasingly pay a premium to attract them because of the potential personal implications.
5. **Audit firm resignations/refusals.** A number of public companies have, for all intents and purposes, been "black-listed" by the big four accounting firms who have resigned or refused their business because the integrity and/or reliability of their accounting controls is questionable. These companies must resort to using lower tier audit firms willing to accept their business that have higher risk tolerances for their audit opinions. Situations like this can, in turn, impact credit ratings, cost of capital and share price.
6. **Impact on the company's share price**. Research in this area is still at a very early stage with somewhat inconsistent results. To date, the only country that has mandated public disclosure of the specifics of material weaknesses in ICoFR detected by management or auditors is the U.S. It isn't at all clear at this point that investors are discounting the price of shares in companies listed in countries that do not require disclosure of the type of information on ICoFR currently mandated in the U.S., and there is at least some evidence that absence of information on ICoFR has no impact or very limited impact on share price. A May 2006 comment paper issued by the Fédération des Experts Comptables Européens on the topic of management reporting on ICoFR reports "There is no evidence of demand for public reports on effectiveness of internal control in Europe" (Section 2 General Comments). This is an area that warrants considerable research to determine how markets react to the absence of information on ICoFR from management and/or external auditors.

7. **Personal philosophy of the company's CEO, CFO and Board of Directors**. The "tone at the top" is regularly cited as key to the issue of reliable external disclosures. The general tolerance of CEOs, CFOs and boards of directors to unreliable external disclosures and the way they personally react when evidence emerges to contrary is a key risk criteria in this area. It is important to note that even companies with excellent tone at the top can suffer instances of materially wrong financial statements because of the inherent limitations of internal control and the fact that some level of risk must be accepted to make a profit and stay in business.
8. **Likelihood External Auditor Opinion on Financial Statements is wrong**. There is a strong implicit assumption in the current U.S. SOX rules that external auditors will render less incorrect audit opinions when they are equipped with better information on the state of ICoFR. This would imply that external auditors should, on balance, have a higher audit opinion failure rate in countries that have not endorsed "SOX-like" rules related to ICoFR. This is a major consideration in the debate over the cost/benefit of the SOX regulatory regime in the U.S. that warrants serious research to prove or refute the assumption.

3.2.3 Risk Criteria – Subsidiary Level

A large percentage of companies, even smaller public companies, have one or more subsidiaries that are consolidated to form the financial disclosures filed with securities regulators. The degree of autonomy and the reporting lines of the personnel responsible for accounts and financial statements of these companies can vary widely. Some of the key risk criteria that impact on attitudes of executives in subsidiaries include:

1. Importance attached to reliable financial statements and accounts by head office. The overall attitude towards undetected errors in accounts at the subsidiary level is communicated in a number of important ways. This includes the importance to reliable accounts and effective ICoFR in job descriptions, the link to reliable accounts and ICoFR to compensation/reward/punishment systems, the rigor of analysis and questions posed by the head office consolidation team to the accounting personnel in subsidiaries, the interest of head office in the frequency and magnitude of errors detected by the external auditors in the course of their audit, the existence and competency of any internal audit function that exists, and others.
2. Personal implications to controllership and local operating management in terms of bonuses and promotions when conscious and/or negligent errors in the accounts filed with head office are identified.

3.2.4 Risk Criteria – Account/Note Disclosure Level

Although the risk criteria that exist at the corporate and subsidiary levels play major roles influencing behavior of senior controllership staff and form the macro level "risk context" for decision making, the risk criteria related to the individual accounts and notes that comprise the financial statements at the subsidiary and corporate levels are also important. These risk criteria impact on the attitudes of the staff that impact directly or indirectly on the reliability of specific accounts and/or note disclosures. The same basic elements listed above influence the perception of accounting staff regarding the importance or reliable financial disclosures.

3.3 Risk Rating & Risk Identification

When tackling the task of applying a true "top-down/risk-based" approach to assessing ICoFR, "assurance contexts" to be assessed must be established at multiple levels and risk rated before deciding where to invest the time and resources required to complete more detailed formal risk/control assessments.

As stated throughout this paper, the most important macro level assurance context for ICoFR is:

Ensure auditor certified financial statements, including the notes, are reliable.

This broad macro level assurance context should constitute the starting point for an entity's macro level risk/control assessment. **This section provides our specific views on how "top-down risk-based" ICoFR assessments should be defined for companies of all sizes to realize the value in their compliance programs**.

Since companies often have multiple subsidiaries and locations, hundreds, if not thousands and even tens of thousands of individual account balances, and scores of note disclosures, a universe of ICoFR assurance contexts cascading from the macro level context must be identified, risk-rated and the conclusions reached and documented for possible review by independent quality assurance staff. For U.S. listed companies the primary independent quality assurance agent for ICoFR is the external auditor. In larger companies the company's Internal Audit department and/or a SOX quality assurance team may also play important roles.

Risk Rating Assurance Contexts for ICoFR

A key step before embarking on more detailed granular risk/control assessments is to identify and risk rate the individual assurance contexts that support the macro assurance context at the corporate, subsidiary and account/note level. A sample of risk rating criteria that can be used when arriving at a composite risk rating on each of the assurance contexts that support the macro level or "parent" assurance context include:

1. Detected error history – external auditor
2. Detected error history – management detected after release of statements
3. Absolute dollar/unit of local currency value/impact of location/account
4. Detected error history – regulators/tax authorities/customers/others
5. Detected error history – internal audit
6. Detected/known errors in other companies in the same business sector
7. Amount of management judgment/subjectivity
8. Importance of account/location to security analysts
9. Importance of account/note disclosure to debt covenants
10. Susceptibility of account to fraud from insiders
11. Susceptibility of account to fraud from outsiders
12. Account/note linkage to the company's reward/compensation system

This is an area where additional research would help refine the accounts/areas in a company that would most benefit from more rigorous and formal risk and control assessment. Some companies have gone so far as to develop weighted numeric risk scoring systems that are then applied to their universe of ICoFR assurance contexts to decide the frequency and extent of analysis and testing each assurance context will receive. **The more these ratings are based on facts as opposed to unsupported guesses and subjective views, the**

better this system will work to actually ensure formal assurance resources are focused where they are most needed. The ratings assigned at this stage have massive and ongoing cost implications because they should, if regulators allow it, influence the extent of risk/control design and control confirmation/operating effectiveness assessments going forward (i.e. the higher the risk rating the higher the assurance cost annuity). If the risk rating system is reliable it should allow for reduced risk and control assessment documentation and testing in areas that have low overall risk scores. These scores should be adjusted on an ongoing, real-time basis as new information emerges or, at a minimum, reassessed annually. Again, the goal is NOT to produce a one size fits all prescription; rather, the goal is to suggest a system that can replace subjective ratings systems that are largely based on the absolute dollar size of account balances.

Identifying Risks to Assurance Contexts Selected for Additional Analysis

Once the assurance contexts to be assessed have been agreed and risk rated, the next step, using the terminology in AS/NZ Risk Management standard, for assurance contexts selected for additional formal assessment is risk identification - "the process of determining what, where, when, why and how something could happen". As a general statement this involves identifying, understanding, and documenting a list of real or potential situations at the "big picture" company level that could cause the non-achievement of the assurance context being assessed. This list should be comprehensive enough that it covers plausible, but not include "far-fetched", risk scenarios. A cardinal rule in risk-based assessments is "MISS THE RISK AND RISK BLOWING THE ASSESSMENT".

Techniques to build a "reasonable" list of plausible risks for an entity-level risk assessment for ICoFR and for more granular sub-elements include the following:

1. **Research and observation** – simply explained, this requires identification of actual situations that have already occurred in other similar public companies that resulted in materially incorrect financial disclosures. Reading newspapers, magazines and journals like Business Week and Compliance Week can produce a solid starting point. A number of relevant websites such as Audit Analytics (www.auditanalytics.com) that track all public companies that have had material control weaknesses and/or restatements of their financial statements are available to assist with this activity. The most dominant risk at the entity level that has emerged from recent scandals is "CEO/CFO/Senior executive instructs or otherwise influences staff to make entries that are fraudulent". Although this may seem to be a somewhat blunt assessment approach, there is no point denying that it was specifically this risk that resulted in SOX being enacted by U.S. Congress. Other common ones include "Compensation system, particularly the company's stock option plan, tempts senior level staff to falsify earnings", "CFO and/or accounting support staff are not current on GAAP", "Staff lack adequate knowledge of applicable federal/state tax law", "Lack of rule clarity how to deal with certain transactions/situations " and others. Every major financial statement misstatement that has been detected around the world, including Enron, WorldCom, HealthSouth, Parmalot, Nortel and hundreds of others, has a "cause of failure".

2. **Company Specific History** – as a company matures a large number of companies, as a result of internal analysis, the work of their external auditor, and the passage of time, realize that they have publicly issued financial statements that were materially wrong in one or more respects. Few companies in the world have continuously produced fault free disclosures prior to the audit/inspection process of their external auditors. Sometimes these situations result in public restatements and, in other

situations, only the existence of internal knowledge on the part of one or more employees that one or more components of the publicly released financial statements were not, in fact, reliable. If these situations are analyzed and a cause of failure determined, it is generally easy to determine the key risks that caused the undetected error. For companies that, for whatever reason, place high reliance on the "end of the line" inspection ability of their external auditors, a key risk is always that "The external audit team assigned doesn't detect and/or require correction of errors that exist in the accounts". Again, the quality mantra of "building quality in, not on" (after the fact inspection) is critical in our view to the goal of cost effective assessments.

3. **Experience of senior level staff** – one of the advantages of growing older and gaining decades of experience in the accounting and control field, often in multiple companies, is that a person gains a broad experience base of what can go wrong and result in major errors in the accounts. This experience base can be used to identify plausible, company specific situations that have the potential to result in material errors in the financial statements.

4. **Industry specific scenario analysis** – this is a technique that can draw on information from the three methods above for inspiration, or be done using "pure imagination" of consultants and/or staff to produce plausible scenarios that could happen that the controls currently in use would not mitigate. The current reforms in the banking sector mandated by Basel II require that all major banks in the world demonstrate that they are regularly doing scenario analysis on the full range of operational risks, including those related to reliable financial statements. This technique is one that can help detect and prevent the next big disclosure disaster that has not happened yet elsewhere (e.g. the use of special purpose vehicles at Enron).

5. **Risk source analysis** – this technique uses a list of potential sources of risk to trigger ideas on possible scenarios that would cause a company's financial statements to be wrong. An example of one risk source framework that can be used is included as Attachment 2. When using aids like risk source lists the general rule is they should be as granular as is necessary to pick-up the significant risks. A risk source list that contains 100 risks sources may not be as effective as one that is more summarized but still causes the assessors to identify a good list of significant risks. The example in this paper demonstrates a risk source framework that has a fairly limited number of risk source categories but has proven very effective as a risk identification tool.

6. **Industry "CHECK LISTS"** – although it is generally better to rely on the methods listed above to generate an industry specific/company specific set of risks, regulators have generally been willing to accept the use of "canned" risk and/or control assessment checklists provided by consultants, external auditors or other providers. When such aids are used care should be taken to try and validate that these assessment aids do, in fact, result in identification of the most probable, company/industry specific risks to reliable financial disclosures. When canned checklists have been employed and produce a conclusion that controls are "effective", it is very important to monitor whether management and/or the company's external auditors are still finding material errors in the draft financial statements. When external auditors find material errors after management and the external audit team has concluded controls are "effective", it is at least prima-facie

evidence that the assessment aid and/or current risk assessment process is inadequate.

(NOTE: It is important to stress that in the U.S. the SEC has repeatedly encouraged companies to begin their risk-based assessment of ICoFR at the top, at the macro/entity level. It is expected that the SEC will provide more details of what they mean by the term "top-down/risk-based" approaches when they issue the new assessment guidance for management they announced in May 2006. The completion date for this new SEC guidance is not currently known.)

A top-down based approach that starts with a macro level assessment on the assurance context of ensuring reliable auditor certified financial statements will often identify where the major holes in a company's ICoFR system without the high expense and massive amount of time required to complete what many refer to as the "BOTTOM-UP" approach to assessing ICoFR. A BOTTOM-UP approach starts by documenting and assessing all the accounting processes that generate or support debits and credits regarded as material in the general ledger. More than a few companies in the first round of SOX did not start at the macro level assurance contexts and did not identify and document the truly "key risks" that history tells us have regularly led to material financial statement errors and the mitigating controls in place to prevent them.

In addition to the type of top-down/entity level assessment described above that starts with the macro level assurance context of ensuring reliable auditor certified financial statements, the process of identifying risks for the more granular assurance contexts that must be assessed to arrive at a supportable conclusion on ICoFR must also be done. Page 11 of this paper outlines examples of the hierarchy of "assurance contexts" that must be risk rated and, potentially, if the risk rating suggests additional formal assessment is warranted, formally evaluated.

3.4 Analyze & Evaluate Risks

Once the assurance context universe has been risk rated and plausible risks to the ICoFR assurance contexts selected for analysis have been identified and documented, the next step is to analyze and evaluate the specific risks. In cases where history clearly indicates a track record of internal or externally detected material accounting errors at the corporate level, or in specific company locations, subsidiaries, departments, and/or accounts and notes, this information needs to be carefully assessed and the relevant risks associated with the errors isolated for special assessment and evaluation treatment.

The process of analyzing risks includes assigning likelihood and consequence ratings to each risk. Generally an attempt should be made to produce these ratings before considering controls (inherent or gross risk ratings). Estimates can also be assigned for the net or residual risk that remains after considering controls although this is often difficult and costly if it is done using facts as opposed to purely subjective opinions. Section 3.5.1 of this paper provides more details on tools available to assign risk likelihood and consequence ratings and generate "risk levels" for each risk to help prioritize the universe of potential risks identified.

Great care must be taken that the risk analysis process does not become too granular, costly and become an industry in itself. The end game is to decide which risks are not currently sufficiently mitigated given the organization's tolerance to accounting misstatements (i.e. these are often identified as "red rated" risks). In real life people and

companies frequently use an experiential, iterative approach that causes them to modify their controls after they are presented with tangible evidence that contradicts previously held views of the likelihood or consequence of a risk (e.g. the risk staff might forge signatures on sales contracts to earn a bonus in a quarter or fiscal year end gets mitigated after a major scandal where this occurs emerges). Using the risk identification techniques outlined in Section 3.3 will help by generating risks that have already proven to be plausible and have, in fact, already resulted in material undetected errors in other public companies. In order to dismiss such risks as irrelevant, a company should be able to explain why their controls would mitigate the risk or be willing to state their current controls might not mitigate the risk and they accept the consequences.

3.5 Treat/Mitigate Risks

3.5.1 Treat Risks Using COSO 1992 Control Criteria

In the October 1987 Report of the National Commission on Fraudulent Reporting (better known as The Treadway Commission after its chairman James Treadway) a key recommendation was that "The Commission's sponsoring organizations should cooperate in developing additional, integrated guidance on internal control." As a direct result of this recommendation, the Committee of Sponsoring Organizations ("COSO"), comprised of the American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA), Institute of Management Accountants (IMA), Financial Executives International (FEI) and American Accounting Association (AAA), developed and issued ***Internal Control-Integrated Framework*** in September 1992 ("COSO 1992"). In COSO 1992 the term internal control is defined as:

"a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

Effectiveness and efficiency of operations
Reliability of financial reporting
Compliance with applicable laws and regulations."

The 1992 framework identified five interrelated components – Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring. An overview of the COSO 1992 framework is included in this paper as Attachment 3. COSO 1992 framework provides narratives of the type of control sub-elements envisioned by the authors of COSO 1992 under each category, but does not have a summary listing or set of definitions of the specific control sub-elements for each category. This issue has been addressed, at least to some degree, in the 2006 COSO Guidance for Smaller Public Companies.

The COSO 1992 framework provides an important caution in the Executive Summary:

*"**Internal control can ensure the reliability of financial reporting and compliance with laws and regulations. This belief is also unwarranted. An internal control system, no matter how well conceived and operated, can provide only reasonable – not absolute – assurance** to management and the board regarding the achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake. Additionally,*

controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs." (page 6)

Unfortunately, it is precisely the type of limitations cited above that caused the enactment of SOX in 2002 and the subsequent regulations issued by the SEC and PCAOB, particularly concerns noted in COSO 1992 related to the difficulty of mitigating breakdowns caused by collusion, management override and faulty judgment. What this important caution is really saying is that, no matter what control framework is in place in a company, there is always some level of residual risk. It is because of the ever present conflict between reasonable assurance at a reasonable cost, and regulatory expectations that want the type of exceptions noted above mitigated that this discussion paper emphasizes the importance of identifying, assessing and consensus agreeing on the acceptability of residual risk status – the risk that remains that a company's current ICoFR system will not prevent auditor certified materially unreliable financial statements.

Although COSO 1992 was not written in 1992 with the intent that it would be used as an ICoFR "how to assessment methodology" (it was written to serve as a ICoFR "integrated framework"), it does provide an overview and discussion of core elements of an integrated internal control system.

Using COSO 1992 for Control Criteria Centric Assessments

To comply with the requirement in current SOX regulations that assessments be done in accordance with a suitable control framework some companies annually, and sometimes even quarterly, have been completing a high level size-up of how their current controls compare to the type of control criteria described in COSO 1992. This approach is sometimes called the "control criteria centric" approach and it is done without explicit and direct reference to specific risks that threaten the macro level objective of reliable financial statements. This approach involves taking the 5 primary COSO 1992 categories and sub-elements that comprise the categories and attempting to determine on a binary basis, whether the company currently demonstrates achievement of the COSO 1992 control elements for ICoFR. An illustration of this approach using an interpretation of COSO 1992 is included as Attachment 11.

To date, few, if any, companies have publicly reported material control weaknesses in their controls relative to any specific COSO control categories or sub-elements. The major challenge when attempting to use the COSO 1992 framework this way is that it was not written with the intent that it would ever be used for "pass/fail" assessments on a specific company's ICoFR effectiveness. The Malcolm Baldrige quality system in the U.S. administered by the American Society for Quality (one of the participating reviewers of this document) is an example of a framework that has been specifically developed to generate repeatable numeric assessments against the quality system evaluation criteria contained in the framework. It is important to note that the Baldrige framework does not define what a "passing" grade should be with respect to a company's quality management system, rather, in the spirit of continuous improvement, it defines quantitatively an organization's progress toward global benchmarks in various categories, categories that are refined and updated for relevance and predictability each year by Baldrige system administrators.

Whether a "control criteria centric" assessment approach that attempts to determine the degree a company conforms to control elements in COSO 1992 is what the SEC has in mind when they use the term "top-down" assessment is not known as of the date of issue of this

discussion paper. It is not an approach that is currently mandated in PCAOB AS2. It is also not a "risk-based" approach (it is control criteria centric), but does reflect a "top-down" emphasis. This issue may be clarified in the new guidance for management the SEC promised in their May 2006 announcement.

Using COSO 1992 for Risk-Based ICoFR Assessments
For companies using the COSO 1992 control framework as an assessment aid for a risk-based ICoFR assessment approach the following steps are recommended:

1. **Develop a universe of ICoFR assurance contexts** that starts with the macro level assurance context of ensuring auditor certified financial statements are reliable at the corporate level, and then moving downwards (i.e." top-down" per the SEC) to include a macro level assessment in all significant subsidiaries that issue standalone financial statements, and on to defining assurance contexts for each of the line items and notes in external financial disclosures. The high-level summarizations line items in financial statements will then have to be further sub-divided to include assurance contexts for all significant GL accounts that comprise the financial statement line items. When grappling with what is a significant GL account or note the overriding decision criteria is encapsulated in the following question - Would a material error in the assurance context being rated result in stakeholders doing something they wouldn't have done had they known the truth? Additional assurance contexts will be required for reliability of IT general controls and can optionally be done separately for the assurance context of preventing fraud related financial statement misstatement, although the fraud related risk component can and should be addressed as an integrated element of the assessment done on all assurance contexts including IT general controls.

2. **Develop and apply a system to risk rate each of the subcomponent assurance contexts identified**. An approach like the one described on page 30 can be used or custom variations developed. This step allows some percentage of the assurance context universe to be eliminated completely for additional formal assessment based on the risk rating generated or identified for reduced scrutiny. If the type of criteria outlined on page 30 is used, even large account balances may be eliminated if they have been error free (both internal and external) and have not been elevated based on other rating criteria such as vulnerability to fraud, industry analyst or debt covenant importance. Companies should agree the assurance context scoring system they develop with their external auditors, and local regulators may also provide input or even specific rules that must be followed. **How far down from the top level assurance context of assessing risks to reliable auditor certified financial statements companies must go, and be able to prove to outsides that they have completed formal risk/control assessments, is a decision on which senior management, security regulators and external auditor standard setters should provide guidance because it has significant cost implications.** Although completing a robust risk assessment on the macro level assurance contexts of reliable auditor certified financial statements may provide 80 or 90% coverage of the major risks that have caused the type of major problems that led to SOX in the U.S., this may not be acceptable to one or more of the key players that input to the assurance context coverage decision, especially U.S. securities regulators and auditor oversight bodies. It is important to note that even 100% coverage of the assurance context universe including formal risk/control assessments on every account in the general ledger will not provide 100% assurance all significant residual risks that could lead to materially incorrect financial statements have been identified.

3. **Identify and analyze risks that threaten the assurance contexts selected for formal review.** For assurance contexts selected for additional formalized risk/control assessment using one or more of the type of risk identification methods outlined in Section 3.3 identify relevant risks and evaluate the risks identified in terms of likelihood and consequence. **A five level numeric likelihood/ consequence rating system is recommended to provide adequate but not excessive granularity. The key is to find a way to rank risks identified in terms of their likely impact on the assurance context.** Risks can be further analyzed in terms of risk source category, the availability and extent of statistical information available on likelihood and/or consequence of major risks, and other criteria. A major trend currently in the risk management field is to supplement subjective judgments on likelihood and consequence with facts and statistics whenever possible. A table with one of the more common systems used to assign "risk levels" based on various combinations of risk likelihood and consequence drawn from a publication titled Guidelines for Managing Risk In the Australian Public Sector is included below to illustrate the concept. Companies can alter the terminology used for likelihood and consequence or substitute simple numeric scores for the likelihood and consequence levels (i.e. 1 to 5), but should maintain the core principle of demonstrating that a reasonable attempt has been made to prioritize the set of risks identified. The main goal of this exercise is to attempt to sort risks in terms of relevance and potential impact to the ICoFR assurance context being assessed.

	Consequences				
Likelihood	EXTREME	VERY HIGH	MEDIUM	LOW	NEGLIGIBLE
ALMOST CERTAIN	severe	severe	high	major	significant
LIKELY	severe	high	major	significant	moderate
MODERATE	high	major	significant	moderate	low
UNLIKELY	major	significant	moderate	low	trivial
RARE	significant	moderate	low	trivial	trivial
SOURCE: Guidelines for Managing Risk in the Australian Public Sector, #22 October 1996					

4. **Identify important controls that mitigate risks with assessable risk levels.** Using the COSO 1992 control category overview shown in Attachment 3 and the supporting COSO volumes that provide more details on the elements of each control category, identify, document and categorize important controls in place that mitigate the risks that have been assigned higher level risk level ratings. (NOTE: the "risk level" is the result of various combinations of likelihood and consequence.) How far down the list of risks identified that matching is done has significant cost implications. In addition to the 5 primary COSO 1992 categories, an interpretation of the COSO 1992 framework is included as Attachment 4. **Other COSO 1992 control sub-element "interpretations" or lists have been developed by companies, external auditing firms, and consulting firms,** however it is important to note that the five member COSO Committee has not formally endorsed any of the many summarized interpretations of the 1992 framework that have emerged over the past 14 years with the exception of their own 2006 COSO SPC guidance that defines 20 principles and sub-attributes. The view may be so long as the approach is "COSO linked", and companies attest in writing that they are ultimately using the core principles in COSO 1992, the use of "COSO 1992 interpretations" is acceptable to the SEC. Further clarification on this point in the upcoming SEC Assessment Guidance for Management would be useful.

Mitigating controls identified for the higher-level risks should be categorized to indicate the applicable COSO 1992 control category. This step helps support CEO/CFO representations that a ICoFR assessment has been done in accordance with a suitable control framework when national regulators require this representation be made. This is also a key step to support the need of U.S. listed companies to prove that an attempt has been made to aggregate control deficiencies to determine if, "collectively", they constitute a reportable control deficiency. If the areas where deficient controls are identified *often* link to a specific COSO 1992 control category it may result in concluding that controls are not effective in accordance with that category of COSO 1992. To date, no guidance has been issued by regulators on the subject of how to do a control deficiency aggregation test related to a control model such as COSO 1992 and PCAOB AS2 provides no specific guidance for auditors on this issue. It is important to note that low likelihood/massive consequence risks should not be ignored since many of the major instances of false or misleading auditor certified financial statements would fall in this category.

5. **Determine whether controls described in step 4 are, in fact, being done as described.** The primary goal of this step is to confirm that controls that have been identified during the risk and control documentation step as mitigators to specific risks are, in fact, being done as described. A simple step that is sometimes overlooked resulting in significant unnecessary costs is to simply ask the person or persons most directly responsible for the control whether the control has been done as described during the period being reviewed. In cases where the control "owner" or "sponsor" indicates the control was done as described, there may be a need, depending on the level of assurance required, to have one or more independent groups verify that the employees with direct responsibility for the control are telling the truth. This step is sometimes called independently verifying "operating effectiveness" or simply "control confirmation. The September 2006 IMA SOX research study indicates that this step is one of the most costly elements for companies that must comply with current SOX regulations. The table below graphically indicates the level of costs that have been incurred testing key controls. Over 92% of respondents rated the testing of key controls as either somewhat costly or very costly.

IMA Research Study: Cost of SOX Compliance-Related Activities (Table 9)

SOX Compliance Activity	Extent to which SOX Compliance Activities are Costly (N=372)			
	Not Costly at All	Not Particularly Costly	Somewhat Costly	Very Costly
1. Creating and Maintaining Process Documentation	0	8% (31)	34% (126)	58% (214)
2. Testing of Key Controls	0	7% (25)	44% (162)	48% (177)
3. Self Assessment by Process Owners	5% (19)	32% (118)	31% (117)	8% (31)
4. Remediation-Related Activities	1% (5)	32% (118)	47% (174)	18% (67)
5. Attestation and Certification	2% (9)	22% (81)	33% (124)	36% (134)
6. Staff Training	2% (97)	39% (145)	45% (166)	12% (44)
7. Investment in New Tools and Technology	6% (23)	31% (114)	34% (128)	16% (60)

Note: In cases where the totals do not add up to 100%, the related activity did not apply to the company.

A simple example of the process of identifying a macro level risk during a top-down assessment and identifying related mitigating controls follows:

RISK: Senior management (CEO and/or CFO) override controls and improperly manipulate/falsify financial statements – Risk Level rating assigned by management: Significant (i.e. extreme consequence combined with a rare likelihood). (NOTE: the company's external auditor might have a very different view on likelihood based on past behavior of management related to earnings management.)

MITIGATING CONTROLS: CEO/CFO Hiring Practices – COSO Category Control Environment, Audit Committee Oversight – COSO Category Control Environment, Confidential concern reporting line – COSO Category Information & Communication, Internal Audit – COSO Category Monitoring, External Auditor audit of financial statements – COSO Category Monitoring.

If the goal is to identify only one or two of the controls as a "key" control to limit the amount of regulatory imposed management and auditor control testing this is a very difficult and subjective decision. In the U.S., the likely key control candidates would be audit committee oversight and confidential concerns reporting mechanism (the company's "hotline") because the U.S. rules do not allow management to view the external audit as a control. In other countries that do not require management reporting on ICoFR and are still tolerant of material undisclosed levels of financial statement adjustments as a result of the work of the external auditor, the key control currently for this particular risk is probably the external audit of the financial statements and the quality of audit staff assigned to do the audit.

Steps would also have to be taken to determine that the controls documented actually were done/completed as described.

The controls currently in use result in some level of effectiveness relative to the assurance context being assessed. **Methods to identify the current residual risk status being produced by the controls in place for any given assurance context are outlined in Section 3.6.** We view the step of identifying and evaluating residual risk status as significantly more important than massive amounts of independent control verification and testing.

3.5.2 Treat Risks Using COSO Smaller Public Company Criteria ("COSO SPC")

In 2004 Don Nicolaisen, SEC Chief Accountant at the time, requested that the COSO committee develop guidance specifically designed to help smaller public companies understand how to apply COSO 1992 during their assessment of ICoFR required by SOX. It was originally expected this new COSO guidance would be available by the summer of 2005 to help non-accelerated filers prepare for the SOX deadline that was looming. As a result of the difficulty of the task, delays in the SOX deadlines announced by the SEC, and other factors this guidance was released in final by the COSO Committee in July of 2006.

The COSO SPC Executive Summary cautions readers that:

> *This document neither replaces nor modifies the Framework, but rather provides guidance on how to apply it. It is directed at smaller public companies – although also usable by large ones – in using the Framework in*

designing and implementing cost-effective internal control over financial reporting.

The 2006 COSO SPC guidance provides 20 "Principles" under each of the original five COSO 1992 categories with a fairly detailed discussion of how each of the 20 principles can be evidenced in smaller public companies (see Attachment 5). These are similar to the 20 control criteria identified by the Canadian CoCo guidance issued in November 1995. Unlike the original COSO framework that indicates on page 21 of the 1994 Executive Summary that setting of objectives is not part of internal control, COSO SPC states: "the internal control process begins with management setting financial reporting objectives relevant to the company's particular business activities and circumstances" (page 11).

Using COSO SPC for Control Criteria Centric ICoFR Assessments

This new COSO guidance provides a more succinct description of the sub-elements that comprise the 5 original COSO 1992 control categories and a better, clearer description of what a company should exhibit to be considered by an assessor to be "effective" on that dimension of control. For purposes of completing "control criteria centric" assessments of ICoFR (i.e. assessing whether a company achieves each of the 20 principles) there is more and better information to help management determine the degree that they currently exhibit the individual control criteria. The Evaluation Tools volume provides detailed tools and checklists that management and auditors can use to arrive at conclusions related to whether the company achieves each of the 20 principles. An illustration of a high level control criteria centric assessment using COSO SPC and a numeric conformance rating system for each principle is included as Attachment 12. The primary difficulty is interpreting what the implications of various COSO SPC principle conformance score profiles mean relative to the chance of a company issuing materially unreliable auditor certified financial statements, and deciding when COSO SPC areas are assessed as having low conformance whether the deficiency or low score constitute a reportable control deficiency under current U.S. regulations (i.e. a significant deficiency or material weakness).

Using COSO SPC for Risk-Based ICoFR Assessments

In general, the same steps for risk-based ICoFR assessments outlined for COSO 1992 above apply. COSO 2006 provides more succinct summaries of key control principles available to mitigate risks at the macro level and, to a lesser degree, controls available to mitigate risks to the more granular assurance contexts such as individual GL accounts, specific note disclosures and IT general control assurance contexts.

For companies using the 2006 COSO SPC guidance for risk-based assessments it offers in the Evaluation Tools volume of the three-volume COSO SPC guidance the following:

1. Ideas starting on page 36 how to complete steps 1 and 2 outlined in Section 3.5.1 of this paper to develop and risk rate the universe of ICoFR assurance contexts.
2. A listing of risks generally relevant when completing macro/entity level risk assessments starting on page 39.
3. Illustrations of risks to specific GL accounts that are considered material and require formal risk/control assessment starting on page 44.
4. If a "process-centric" approach to ICoFR risk assessment has been used for more granular account assurance contexts it provides examples of how to map from supporting business processes to financial statement line items starting on page 37. To form an opinion on acceptability of residual risk related to a specific account or note disclosure decisions must first be made on reliability of all supporting processes.

That information then forms part of the information on the residual risk status related to the specific end result assurance context.

5. To determine where IT general control assessment assurance contexts should be used it illustrates how to map from business processes that impact on the financial statements to supporting IT infrastructure.
6. If a process-centric assessment approach has been used that includes the concept of account "assertions" it illustrates, starting on page 49, how to link business processes and account assertions to specific risks and controls. (NOTE: We have recommended against using the term "account assertions" as a core element of the assessment methodology because it cannot be used when assessing assurance contexts that do not relate to ICoFR.)

The ICoFR top-down/risk-based assessment approach proposed in this draft includes the following recommendations and approaches that we believe differ in focus and/or approach from the COSO frameworks described thus far:

1. **Companies identify and focus significant attention on the current residual risk status** related to all ICoFR assurance contexts analyzed including macro level assessments, external statement line items and notes, and supporting general ledger accounts. We believe that a residual risk focus combined with a risk-based assurance context priority rating system has the best potential to control long-term compliance costs and add maximum value to the company.
2. Companies **continuously identify and monitor the current error rate that exists for all relevant ICoFR assurance contexts** by identifying and analyzing errors determined by external auditors, outside regulators, customers, suppliers, and internally by management (i.e. the error or non-conformance rate). This recommendation is akin to doctors monitoring for symptoms before proceeding to more rigorous and sometimes intrusive tests. The national economy of a country would be massively negatively impacted if a law was passed that all residents of that country must undergo extensive physical examinations and hundreds of tests related to their health regardless of their symptoms, age, sex or specific risk factors.
3. **Identification and candid acknowledgment that some risks are not mitigated in whole or part with specific formal auditable controls** because of company size, resource constraints, industry specific factors, and other reasons. These residual risks must be communicated to the company's external auditors so they can appropriately modify their audit plan and still provide a high level of assurance the financial statements are reliable and "fairly stated".
4. ICoFR **must also include an assessment of risks and controls that ensure the reliability of financial statement note disclosures.** Note disclosures provide important information that is relied on by a range of stakeholders and are explicitly included in current SEC ICoFR assessment requirements. An IMA research study released in September 2006 clearly indicates a significant number of companies did little or no assessment of risks and controls related to their financial statement note disclosures with the explicit or implicit agreement of their external auditors. (It is important to note that the status of a company's stock options is communicated primarily through financial statement note disclosures. This area is currently under heavy scrutiny by the SEC.)
5. No specific guidance is provided in the control-centric frameworks described thus far on how to identify relevant risks to the various assurance contexts. This discussion paper **proposes some specific techniques that can be used to identify and prioritize risks to the full range of assurance contexts.**

3.5.3 Treat Risks Using CARD®model, A COSO Linked Framework

Attachment 8 to this discussion draft is an example of a public domain control model called CARD®*model* that is linked to the original COSO 1992 and COSO SPC frameworks and has been referenced in a number of Institute of Internal Auditor and IMA publications. CARD® stands for Collaborative Assurance & Risk Design. It uses 8 control categories versus the 5 primary control categories in COSO. This model puts higher importance on "Commitment", "Indictor/Measurement", and "Process Oversight" controls relative to the attention given in COSO 1992. Each of the eight control categories in this model relates to an element of an organization's control framework. Beneath each of the 8 categories there is a "menu" of the specific control elements that an organization could use to achieve the core control category objective. Supporting each sub-element of control is a "trigger" question that helps people understand the purpose of the control. This framework has been developed and tested over the past 20 years and draws on COSO 1992 and the other national frameworks covered in this paper, as well as the Malcolm Baldrige Quality framework, and other control models including the Modern Comptrollership framework developed in the Canadian public sector. All control elements in COSO 1992 and COSO SPC frameworks are included in this COSO linked framework although they are organized under different control category headings.

This reference aid can be used to identify existing or possible controls available to mitigate a particular risk and indicates to readers at a glance the mix of the type control design elements that are currently being used (e.g. a control design that lacks Measurement/Indicator controls or Commitment controls).

An illustration of how this CARD®*model* methodology can be used for the same example used in the COSO 1992 section follows:

RISK: Senior management (CEO and/or CFO) override controls and improperly manipulate/falsify financial statements – Risk Level rating assigned by management: High (i.e. extreme consequence with a moderate likelihood).

MITIGATING CONTROLS: CEO/CFO Hiring Practices – Element 4.4 Capability and Continuous Learning, Audit Committee Oversight – Element 8.6 Process Oversight, Confidential concern reporting line – Element 6.7 Indicator/Measurement, Internal Audit reviews – Element 8.2 Process Oversight, External Auditor audit of financial statements – Element 8.3 Process Oversight, 6.1. Results and Status Reports/Reviews.

The CARD®*model* framework was specifically designed to help people with the task of identifying the controls currently in use that mitigate specific risks identified to a given macro or micro level assurance context and help them to understand what controls they could use if current performance or error rate for any assurance context is unsatisfactory. One of the key benefits of this framework is that users only need to have the three reference documents included as Attachment 8 to this paper as a reference aid when attempting to identify and/or categorize existing and potential mitigating controls.

3.5.4 Treat Risks Using Canadian & U.K. COSO Linked Criteria

Attachments 6 and 7 of this paper include an overview description of the Canadian "CoCo" and U.K. Cadbury/Turnbull control frameworks. In both instances the original control framework was issued in the mid 1990s and some years later additional guidance was issued on how to complete control assessments. Both frameworks were intended to be used for the full range of internal control assessments and provide very little specific guidance how they can be used to assess ICoFR. The SEC has indicated both of these frameworks are

acceptable for use for SOX assessment but it isn't clear if the SEC means the control frameworks only, issued in the 1994/95 timeframe which are most similar to COSO 1992, or the guidance issued some years later describing how to go about assessing control which are more similar to the 2006 COSO SPC. **From a technical standpoint, the U.K. Cadbury/Turnbull guidance has very few real differences from categories and elements in COSO 1992. The Canadian guidance is quite different from COSO 1992 as the decision was made by the CoCo Committee to go with a 4-category/20-attribute framework that focuses more on the people dimension of internal control.** CoCo was also designed to more easily accommodate assessments at the macro/entity level as well as more granular assessments required for ICoFR application on individual financial statement accounts, general ledger balances or note disclosures.

In practice, the major public accounting and consulting firms have shown very limited willingness to support anything other than the COSO 1992 framework for SOX assignments even when the SEC registrant companies are headquartered in the U.K. or Canada. The Canadian Institute of Chartered Accountants that sponsored the development and launch of the CoCo control framework has not encouraged the use of the CoCo framework in Canada for purposes of the new ICoFR management reporting requirements mandated pursuant to Multilateral Instrument 52-109. The U.K. has not enacted any laws or regulations that require management reporting on ICoFR at this point, but has endorsed a "comply or explain" regime related to a much broader set of risk and control governance criteria set out in a document called the Combined Code. Revised guidance on complying with the Combined Code was issued in the U.K. by the Financial Reporting Council in October 2005. In that guidance the authors raise the very real concern that complying with the U.K. Turnbull guidance is not likely to actually result in complying with the assessment guidance issued by the SEC and PCAOB, regardless of the fact that the U.K. Turnbull guidance has been cited by the SEC as a "suitable" assessment framework. In the Conclusion section of "The Turnbull guidance as an evaluation framework for the purposes of Section 404(a) of the Sarbanes-Oxley Act" issued December 16 2004 it states:

Whilst the Turnbull guidance is a suitable framework for the purposes of S404(a) of the Sarbanes-Oxley Act, nothing in the Turnbull guidance reduces SEC registrant's obligations to comply with US laws and regulations. (page 11)

The reality is that using the U.K. Turnbull or Canadian CoCo assessment criteria and guidance would not, in many respects, meet the type of highly prescriptive expectations currently set out in the U.S. in PCAOB AS2. This is likely one of the reasons that so few firms and advisors have recommended the use of any control framework other than COSO 1992.

3.5.5 Treat Risks Using COBIT/ISO 17799/ITIL

Common risks that emerge when identifying and evaluating risks to the overall reliability of the financial statements and the line items and notes that comprise them relate to the following broad areas:

1. Software program do not correctly calculate/allocate/handle transactions that impact on the financial statements.
2. Accidental or intentional unauthorized/inappropriate modifications to software programs.
3. Unauthorized/inappropriate/fraudulent modification of data in the system that is used to calculate/process accounting entries.

4. Unauthorized/inappropriate/fraudulent creation and submission of data to the accounting system.
5. Spreadsheets used to feed or produce accounting entries or notes are inaccurate/unreliable/not secure.

The controls that mitigate the type of risks identified above are most generally called IT general controls.

For U.S. listed companies PCAOB AS2 mandates that external auditors must independently assess IT general controls that impact on the financial statements when completing SOX 404(b) assessments. In the absence of any guidance from the SEC on the subject management has, by extension, used the general IT controls assessment requirements outlined in PCAOB AS2 related to IT general controls. The area of IT general controls external auditor evaluation has been an area that has attracted a high number of complaints with a common theme that registrants believe that their external auditors and/or consultants have required an excessive amount of work on this dimension of control resulting in high ongoing costs.

The September 2006 IMA SOX research study titled "COSO 1992 Control Framework and Management Reporting on Internal Control over Financial Reporting: Survey and Analysis of Implementation Practices" discloses that the majority of companies indicated that they used the COBIT framework issued by the IT Governance Institute to assess the IT dimension of ICoFR for SOX. (See table below.) An ISACA research study (April 2006) collaborates this finding even more definitively. Research indicates that virtually all of these companies indicated in their SEC filings that their ICoFR assessments have been done in accordance with COSO without mentioning that COBIT was used for the IT dimension. To date the SEC has not indicated that COBIT or any other IT controls assessment framework is a "suitable" assessment framework for purposes of Section 302 or 404 control assessment work. Companies that did indicate that they were using COSO 1992 for IT general control work did not indicate how they used it. COSO 1992 makes only brief mention of controls over information systems in the control activities chapter but provides very little, if any, guidance how to assess their effectiveness. Further, in the 2004 "IT Governance Global Status Report" authored by PwC and ITGI, they state "COSO does not adequately address IT control requirements within the framework. Sarbanes-Oxley provides an opportunity to position CobiT as the keystone framework for IT management and control." While Figure 69 of that document presents a detailed mapping of COSO and CobiT, the authors acknowledge "whilst intellectually stimulating, it could be argued that the existing mapping is too complex to have a clear impact on executives and boards."

IMA Research Study: Frameworks Used to Assess Effectiveness of Internal Controls over IT (Table 35)

Type of Control Model	# of Responses (N = 373)	% of Total Responses
1. CObiT	193	51.7%
2. ITGI-A subset of the CObiT	36	9.7%
3. COSO 1992	165	44.2%
4. COSO ERM	7	1.9%
5. ISO 17799	14	3.8%
6. Uncertain	72	19.3%

Attachment 9 to this paper includes an overview of COBIT 4.0 control domains and processes. The elements of COBIT that are potentially relevant to ICoFR are identified as "Primary support in relation to SOX" or "Secondary support in relation to SOX". These

designations were assigned by this paper's primary author and have not been reviewed or endorsed by the committee responsible for COBIT or the IT Governance Institute. The ISO 17799 IT security framework and COSO ERM are the only "risk-based" assessment frameworks listed in this IMA survey question. COBIT is not technically a "risk-based" or "risk-centric" assessment framework but can be used as an excellent reference source for guidance on appropriate controls to manage IT risks. It is interesting to note that almost 20% of respondents in the September 2006 IMA SOX research study indicated they didn't know how their organization had dealt with the PCAOB requirement to assess the effectiveness of IT general controls.

At a macro level it is important to point out that only a small percentage of the major financial statement reliability problems and scandals that have occurred around the world were directly and solely linked to problems related to IT general controls. No records are available to determine what percentage of external audit opinion errors were caused primarily by IT related control deficiencies. (Note: there is very little published research on the subject of root causes of audit failure because of the inability of researches to access the necessary information.)

Countries that want to adopt a "risk-based" approach to IT general controls related to ICoFR should consider evaluating the benefits of using a combination of the residual risk centric assessment methodology outlined in this paper together with COBIT, the ISO 17799 framework (*Information technology – Code of practice for information security management),* and the ITIL framework developed by the Office of Government Commerce in the U.K.

The ISO 17799 guidance on page IX states:

"Risk assessment is systematic consideration of:

a) the business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;
b) the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerability, and the controls currently implemented.

A precedent setting paper calling for convergence and integration of competing IT standard setting bodies titled ***Aligning COBiT, ITIL and ISO 17799 for Business Benefits: A Management Briefing from ITGI and OGC*** suggests that:

Every organization needs to tailor the use of standards and practices, such as those examined in this document, to suit its individual requirements. All three can play a very useful part – COBIT and ISO 17799 helping to define ***what*** *should be done and ITIL providing the* ***how*** *for service management aspects.*

It is clear from the September 2006 IMA SOX research study survey points, the points raised in the COBIT/ ISO 17799/ITIL integration/alignment paper, and conflicts in the current U.S. regulatory guidance and reporting requirements related to how to approach IT general controls assessment that there is an **urgent need for more clarity on how management should approach this area** in U.S. listed companies. Companies are optimistic that the SEC will clarify for U.S. listed companies how the area of IT general controls should be approached in their promised guidance for management.

3.5.6 Treat Risks Using the OCEG Foundation Framework

For risks that relate directly to business ethics and the ethics of individual senior executives Attachment 10 is a framework that has been developed by the Open Compliance & Ethics Group. It provides considerable detail on tangible methods companies can use to mitigate specific ethics and legal compliance risks. Considerable work and input has gone in to the development of this framework and it has undergone a very rigorous exposure and comment process. This framework is particularly relevant to the type of risks that caused SOX to be enacted in the U.S.

3.6 Identify, Assess & Report On Residual Risk Status

Once the assurance contexts to be assessed have been decided on, relevant risks identified, prioritized and evaluated, and the mitigating controls for those risks identified and documented, the last step is determining the current "Residual Risk Status". This sequence can also be reversed wherein a company monitors the residual risk status for a given assurance context and only completes a formal risk and control assessment to determine the cause when the residual risk status information indicates a problem. The option of monitoring key performance indicators and key risk indicators prior to completing full assessments is not available to U.S. listed companies that must comply with the current SOX regulations for sections 302 and 404.

Residual risk is defined in AS/NZ 4360 Risk Management standard as "the risk remaining after implementation of risk treatment". For ICoFR this is the risk that remains financial statement line items and/or notes are, or could potentially be materially wrong in whole or part.

Residual risk status is a collection of information that helps management and audit committees decide whether the residual risk related to the goal of reliable financial disclosures is, or is not, acceptable. As noted earlier in this discussion draft, the options to manage risks to reliable financial disclosures include mitigating risks through controls, sharing or transferring risks in some way, avoiding risks, or accepting the risk and the consequences that might flow from risks accepted. A simple example of risk acceptance is an audit committee that has decided that existing accounting personnel and controls might not produce reliable financial statements for one or more reasons and relies on the company's external auditor to find errors and get them corrected prior to release of the financial statements. The chance of an undetected error is higher in this situation.

In the methodology proposed in this draft we recommend creating a composite snapshot of residual risk status for selected assurance contexts. Residual risk status is comprised of some combination of the type of information below. In some cases all that may be known at a point in time are control concerns, areas where controls are or could be ineffective mitigating one or more risks. In other situations, indicator data may be available indicating fact based information on how well the existing control design or operation is working. (A positive example of indicator data is a public company where the external auditor has found no material errors in the financial statements prepared by management for 3 consecutive year-ends and the company has never had a restatement of its accounts in its history.) It is important to note that the key is that management and audit committees make prudent decisions on whether to change or modify the existing ICoFR control design/operating effectiveness level or leave the control framework unchanged.

Types of Residual Risk Status Information

Concerns – (also known as issues or review findings) these are real or potential situations that have been identified where the current controls in place do not, or might not, mitigate one or more risks in whole or part. Management must then decide whether the situation represents a Concern-acceptable or a Concern-unacceptable. In many companies concerns explicitly or implicitly deemed acceptable are often not documented. An example is an accounting balance that involves estimates that requires a high level of judgment and experience. A risk is inexperienced staff making the estimates make serious mistakes. The current employee that is making the judgments is new to the industry and the position and lacks knowledge and experience. This creates a residual risk concern. In the absence of adding other compensating controls this produces a residual risk concern that is either acceptable or unacceptable to senior management. We encourage companies to document residual risk concerns that they elect to accept at a point in time because new information may emerge and a concern that was acceptable at a point in time may not be down the road because of differences in circumstances and/or risk tolerance. It is very important that external auditors are made aware of situations where the controls may not mitigate one or more risks that threaten the reliability of one or more accounts or notes. In some percentage of these situations they can elect to increase the substantive testing work they do to confirm the reliability of the accounts in question with the end result that the goal of reliable auditors certified financial statements is still achieved. In other situations, it may not be possible or be very expensive to reduce the risk of financial statement error. An example of this type of situation is when accounting program change controls or data access controls are unreliable and the impacted account balances are not amenable to reliable external auditor confirmation (e.g. whether a program functioned consistently and correctly throughout an entire accounting period without unauthorized changes). Auditors are placed in a very difficult situation when general IT controls are seriously deficient because audit theory dictates that extensive work must be done to achieve a high level of audit assurance.

Indicator Data – this is information about how well a given assurance context is being met. (NOTE: This is not whether controls were performed as described but rather the degree to which the controls are actually mitigating risks to the assurance context being assessed.) An ICoFR example is a company discloses in their 10K that they have a profit before tax of $100 million. Their auditor has given a clean opinion on the financial statements and an opinion that ICoFR is effective in accordance with COSO. It is subsequently determined that $30 million of inventory shown on the balance sheet does not exist and the financial statements for the period must be restated. The assurance context is that inventory balances are reliable. The new information that has surfaced helps illustrate how well the controls worked to mitigate one or more risks. For an individual account balance indicator data could be a material error discovered by the external auditor after management has signed off on the financial statements, or information that emerges in a subsequent accounting period and management is now aware that statements filed with the SEC contained some level of material error. Other less obvious examples might be an abnormal number of credit notes that must be issued in the first quarter of the year because the customers deny that they actually ordered the goods that were included in the prior period's sales. This is indicator data that the assurance contexts of reliable accounts receivable and sales were not met in part for that year-end.

Impact Data – this is information that helps decision makers understand the consequences that will or could flow from specific errors in the company's financial statements. Errors that impact only on classifications within similar balance sheet or income statement classifications are generally not as serious as balance sheet errors that impact on the

income reported. Errors in some balance sheet accounts or notes to the financial statements however could have an impact on debt covenants triggering a loan repayment, credit rating review or other major consequences. An example would be errors in a note disclosure that is used extensively by security analysts that track a particular industry. The likely impact of financial statement errors is an area that is complex with few hard and fast rules. Investors sometimes appear to have fairly high tolerance to certain types of accounting errors but react drastically to others. A related area that is currently being debated on a global level is what type and/or size of error should result in a restatement of prior period financial statements.

Impediment Data – in some situations there may be risks that threaten the reliability of accounting disclosures that are very difficult, expensive or even impossible to mitigate to a tolerable level because of one or more circumstances. An example might be a company that is developing new products or services that have not existed previously anywhere in the world. Since there is no historical/corporate memory or awareness of these risks it can cause material accounting errors. Another example of an impediment would be a legal decision handed down or an out of court settlement reached late in an accounting period in a case a company in the same industry is involved in that has the potential of materially impacting a company's valuation of one or more accounts. It may not be possible or practical to access this information on a timely basis. A very simple example may be a situation where a majority shareholder has dictated that an unqualified individual that lacks the necessary knowledge or skills fill key accounting positions like CFO or Controller. The only viable mitigation for the type of risks that would flow from this situation is the skill of the external auditor finding and correcting errors and/or highly competent personnel in the controllership department.

Transfer/Risk Sharing Information – this is information about situations where some or all of the responsibility to mitigate risks has been shared or contractually transferred to another party. For ICoFR an example is outsourcing all responsibility for the company's pension fund management including the design and operation of controls to ensure accounting balances are reliable. Under current U.S. rules this may require that the organization that is doing the accounting have a "SAS 70 review" of their controls. Determining that one has been done may, or may not be enough to discharge a company's responsibility to ensure their own financial statements are reliable.

3.7 Management Quality Assurance Processes

The central goal of a reliable system of ICoFR should be to produce materially fault free financial statements for the company's external auditor to review, much the same as the goal of factory production lines should be to produce fault free product for the inspectors at the end of the line before the products are shipped. By extension, this goal can be alternatively stated in a different way as **"Minimize financial statement rework"**. Securities regulators in all countries around the world should consider how much flexibility management is allowed to accomplish the goal of producing materially fault free financial disclosures and the level and type of financial statement "rework" as a result of external auditors involvement that is tolerable without any impact on management's control effectiveness claims. This is a **particularly important issue for smaller public companies** where the amount of rework between the production of management's draft financial statements and the final statements varies widely and can be substantial.

Regulators must also routinely reassess whether they are satisfied with the current capability of external auditors that audit the accounts of regulated companies under their

jurisdiction to identify material errors in financial statements. The ability of external auditors to identify material faults in the financial statements produced by management is a critical key indicator of how well managements ICoFR quality assurance systems are working. When situations emerge where management and external auditors have both concluded that ICoFR is “effective” or, alternatively, not reported any major residual risks, and material errors in the accounts and/or notes are still detected during the audit this should be viewed as a flag and a detailed reassessment undertaken of the reliability of ICoFR assessment methods used by both parties. Management should have their own early warning systems to identify reliability problems in their ICoFR systems and make every effort to minimize the frequency of auditor detected material errors in financial statements.

In countries where securities regulators still accept situations where the external auditor routinely finds material errors in draft financial statements and requires management correct them before financial statements are released (i.e. before the product is filed with regulators) the rules of the game are significantly different than in countries where the regulators has mandated public admissions by management and/or auditors of ICoFR deficiencies in most instances external auditors identify material errors in the accounts and notes.

We suggest that **securities regulators look to the quality management profession and learn from the extensive work done over the years** on ways to help management improve the reliability and consistency of quality systems. The Six Sigma approach to costly fault identification and correction may be a particularly fruitful area of study in terms of applicability to ICoFR. The objective is NOT to prescribe a one size fits all approach, but rather to integrate the proven principles from the quality profession applied in practice globally over the past several decades. ASQ, the American Society for Quality and the administrators of the Malcolm Baldrige Quality Award, is available to assist in this regard.

3.8 Process Documentation & Record Retention

The amount of process documentation and records that must be created and retained to demonstrate that a company has met statutory and/or civil duties of care with respect to formal assessment of ICoFR is highly variable and is almost always directly linked to legal and regulatory requirements, including the risk of a criminal or civil law charge alleging negligence. Companies that have already had to comply with the U.S. SOX regulations have reported high variability in the amount of detail their external auditors have demanded in the way of supporting documentation. To date there have been no reported instances where an external auditor firm has been publicly censured by the PCAOB for having done an inadequate or negligent job assessing the process used by management to assess ICoFR or independently conclude and report on the effectiveness of internal control, although this type of situation may start to emerge as time goes on. It is only a matter of time before a management team and their auditors certify that ICoFR is effective and subsequently it is proven the audited financial statements are materially wrong and a law suite is launched. Regulatory sanctions and legal jurisprudence will slowly begin to clarify the very difficult question of “how much is enough”. Certainly there have been no reported cases of an external audit firm that has been sanctioned by the PCAOB for demanding too much ICoFR assessment or testing work however this may occur in the future.

It is expected that for U.S. companies this is an area the SEC will provide some much needed clarification when they issue the ICoFR assessment guidance for management they have promised. The PCAOB is also expected to release additional guidance on the approach external auditors should take once management has begun to implement the type of “top-

down/risk-based" assessment promised by the SEC. As a matter of general common sense the amount of documentation should be adequate to convince an independent and knowledgeable third party that all steps currently required by law and regulation have been completed in a reasonable manner. The more ambiguity on what the law requires the more difficulty there is determining how much is enough. When laws clearly indicate the type and amount of ICoFR assessment work it is up to management's discretion there is much greater flexibility.

For public companies listed on exchanges in countries other than the U.S. there is currently little guidance available in the area of mandatory documentation requirements for management claims on ICoFR or the broader risk management capability. Canada has announced that management of public companies listed on Canadian exchanges must begin in 2006 to make formal representations on ICoFR. No specifics have been released on what support management should have to support such claims other than stating the regulators reserve the right to request that management produce the support for their representations if asked. Canadian regulators have explicitly indicated that external auditors should not associate and sign audit opinions on financial statements of companies where they believe management's public representations on ICoFR are false or misleading.

It is important to note that type and amount of documentation required is directly linked to the ICoFR assessment methods and approaches mandated or approved by regulators and/or auditor oversight bodies. The amount of documentation for high-level control criteria centric ICoFR assessments would be a fraction of the documentation required for process/control centric/assessment currently mandated in PCAOB AS2. The lowest amount of formal documentation would be if regulators were satisfied with a macro level risk and control assessment on the macro level assurance context of ensuring reliable auditor certified financial statements.

4. GLOBAL REGULATORY CONSIDERATIONS

Securities regulators and auditor oversight bodies around the world have been watching the U.S. "SOX experiment" with great interest. Although SOX has created a massive amount of criticism and debate and is still in a state of significant change and evolution in the U.S. The really fundamental questions everyone should be asking, and actively searching for answers on, include:

1. Are audit opinions issued on the financial statements of companies that are in full compliance with regulations related to SOX Sections 302 and 404, on balance, more reliable than:

    a) Auditor opinions on financial statements of U.S. companies that do not yet have to fully comply with SOX Section 404 regulation such as non-accelerated filers and private companies?

    b) Auditor opinions on financial statements of public companies listed in other countries that do not require "SOX-like" mandatory management assessment and reporting on ICoFR and/or mandatory auditor assessment of ICoFR?

2. Do investors and other stakeholders, including credit rating agencies, lenders, regulators in sectors like banking and insurance, and others, believe that financial statements produced under the SOX ICoFR assessment and reporting regime are, on balance, more reliable than other audited financial statements? Point 2 is linked to the amount of publicized evidence that supports the hypothesis in point 1.

If the answer in all cases noted above is "NO", the intellectual validity and cost/benefit justification of the current SOX process must be seriously questioned. If the answer in all cases is "YES", all securities regulators around the world that want to protect the efficiency and increase the attractiveness of their capital markets internationally should be actively considering enacting mandatory management reporting on ICoFR with some form of auditor assurance that management representations on ICoFR are reliable.

Key issues that all securities regulators around the world should consider if enacting or modifying laws and/or regulations related to mandatory management reporting on ICoFR are listed below. Comments based on research undertaken by the IMA and FEI related to SOX and COSO and some general observations on each issue follow.

1. FORM AND CONTENT OF MANAGEMENT REPRESENTATION
2. FORM OF AUDITOR ASSURANCE ON ICoFR
3. GRADING CONTROL DEFICIENCIES
4. MANDATORY ICoFR ASSESSMENT METHOD(S)
5. MANDATORY USE OF ONE OR MORE CONTROL FRAMEWORK/CRITERIA

1. FORM AND CONTENT OF MANAGEMENT PUBLIC REPRESENTATION ON ICoFR

When U.S. Congress enacted SOX in 2002 it called for each issuer to file a report on internal control that includes ***"an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting."*** To date in the U.S. this

Section of the Act has been interpreted by the SEC and PCAOB to mean that management must report a binary, effective/not effective, conclusion on ICoFR. The SEC has mandated that the existence of even one "material weakness" must cause management to report publicly that the company's entire system of ICoFR is ineffective. This decision is at the root of tens of thousands of hours of acrimonious debate and has contributed to the massive costs that have been incurred to date. Some specialists in the field believe it may be creating an unrealistic perception of what ICoFR can, and cannot, achieve.

Our reading of the Act suggests that U.S. Congress was very interested in taking steps to ensure that management takes full responsibility for identifying and reporting on serious control deficiencies in ICoFR to the company's audit committee and external auditor. We believe that this is an entirely appropriate focus for all capital market regulatory reforms around the world. We believe that the focus of public representations from management on ICoFR should be to acknowledge that a) they are responsible for creation and maintenance of a reliable system ICoFR, and b) they have created and maintain a reliable system to identify and report serious deficiencies in ICoFR to the company's audit committee and external auditor. This is not the same as a requiring a binary representation that ICoFR is "effective" or "ineffective". **A sample management representation on ICoFR that we believe would lead to greater cost efficiencies in this area while still producing reliable information on the current state of ICoFR and reliable auditor certified financial statements is included as Attachment 13**.

It is important to note that many U.S. listed companies have been forced to publicly report their ICoFR system is ineffective at the same time the company's external auditor has certified that the company's financial statements are reliable and "present fairly" the position and results of operation. We believe this situation can result in user confusion, particularly when the control deficiencies being reported are very serious and pervasive. Users appear to be most interested in knowing whether the financial statements are reliable and, by extension, that the audit opinion provided on the statements is reliable.

Moody's, a leading credit agency, has publicly questioned the ability of external auditors to "audit around" certain kinds of control deficiencies. Based on the September 2006 IMA SOX research study and other sources, we do not believe that current ICoFR standards and assessment frameworks are able to produce repeatable conclusions from management or auditors on overall ICoFR "effectiveness". There is at least some evidence that suggests that there are some significant inconsistencies in the conclusions being reached by external auditors when asked to provide their own opinion on whether controls are, or are not, effective. We believe that when external auditors are fully apprised of areas of ICoFR that may be deficient they are better equipped to adjust their audit plan accordingly and provide more consistently reliable audit opinions. Canadian external auditors will face very difficult decisions in cases where management of Canadian public companies publicly claim their ICoFR system is effective under new requirements in Multilateral Instrument 52-109 at the same time their audit has revealed major errors in the accounts and/or notes requiring adjustments by management before auditors are willing to certify the accounts.

2. FORM OF AUDITOR OPINION ON ICoFR

Section 404(b) of the Sarbanes-Oxley Act of 2002 states **"each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the**

issuer." Currently in the U.S. this has been interpreted to mean that external auditors should give a three-part opinion - an opinion on the financial statements, an opinion on the process used by management to assess and report on ICoFR, and an opinion on whether they believe ICoFR is effective. The Act goes on to state: "**Any such attestation shall not be the subject of a separate engagement".** The involvement of the external auditor with management's representation is one of the most controversial elements of the current SOX regulatory regime and has led to a range of problems. Canada, the U.K. and Europe, after careful study, have both rejected the current form of auditor association currently required in the U.S.

Given our suggestions above on the most appropriate form of management representation **we suggest regulators that have decided to implement some form of mandatory management reporting on ICoFR seriously consider requiring auditors give an opinion on the system management has in place to identify and report serious ICoFR control deficiencies to the company's audit committee and external auditors, but not be required to provide their own binary and subjective view on whether ICoFR is effective (i.e. a "two part opinion").** We recognize this recommendation is not in line with some of the current thinking in the U.S. in this area. To limit the subjectivity in this area, external auditor's could be required to use the frequency and magnitude of accounting and note adjustments that are a direct result of their audit as one of the considerations when deciding on the "grade" to assign to management ICoFR efforts. This could be as simple as an alpha grading system – A, B, C, or D. Companies that have been assigned a grade of A on ICoFR work should have a significantly lower audit cost than a similar company that has received a grade of D. This type of system would provide positive incentive for management to improve the quality of their ICoFR systems.

The Institute of Internal Auditors (IIA) currently requires that internal auditors that want to conform to the standards set for the profession assess and report on the quality of management's risk management systems. The work the IIA has done in this area could form the basis of new external audit standards on how to grade and report on a company's system to assess ICoFR. Chapter 8 of IIA Handbook Series *Implementing the Professional Practices Framework* should be consulted for more details.

3. GRADING CONTROL DEFICIENCIES

U.S. listed companies are currently expected to grade deficiencies in to three buckets – low level control deficiencies, significant deficiencies and material weaknesses. Experience gained to date as a result of the SOX ICoFR regulatory process indicates that grading control deficiencies identified by management or external auditors is one of the most problematic elements of a ICoFR assessment and reporting regime. Current SEC/PCAOB rules in the U.S. require that management determine when a deficiency in control is such that there is "**more than a remote likelihood**" an error in the financial statement balances or notes could occur that is "**more than inconsequential**". This approach to grading guidance has proven in practice to be very difficult to apply and has resulted in heavy criticism (particularly from the smaller company community) and public reporting of some relatively low control issues.

A simple example of deficiency grading would be CFO/Controller team that has a track record of producing draft financial statements that contain material errors identified by the company's external auditors. The primary cause is accounting staff not having or not staying current on their knowledge of GAAP. This type of situation may be the case in more than a few smaller public companies because smaller public companies, often for

good reasons, before SOX relied on their external auditors that focus on GAAP compliance to compensate in this area. Since U.S. regulators have decided, at least thus far, that a company's external auditor can not also serve as an accounting consultant (e.g. for "readiness" mode in SOX implementations), and given the track record of detected material errors traced to this weakness, it is fairly clear that this situation meets the current SEC/PCAOB definition of a material control weakness. A situation that is less clear is one where the company uses internally developed or modified accounting systems that were developed with very weak systems development and change controls over the past 20 years. Determining whether there is "more than a remote likelihood" that this type of control weakness could lead to an undetected error that is "more than consequential" is considerably more difficult in practice, particularly if the external auditors have never found an error to date in the accounts that can be traced to errors in the software logic.

A real life illustration of this type of control deficiency is one of Canada's largest banks recently acknowledged that their mortgage accounting systems had incorrectly calculated mortgage interest on tens of thousands of customer mortgages for a number of years undetected by management or the bank's external auditors. This bank had been asserting in SEC filings that their ICoFR was "effective" and their external auditors had supported that conclusion. Although an argument could be advanced the overcharge was immaterial, the broader implications to the entire portfolio of the bank's products impacted by computer systems is a much bigger issue.

The SEC has indicated some willingness based on considerable feedback they have received on the issue of control deficiency grading to revisit the guidance for management in this area.

Rather than using the type of grading approach currently mandated in the U.S., another option is a more flexible control deficiency grading system developed and tested over the past decade that has proven reasonably practical is included as Attachment 14. A major benefit of this grading system is that it can be used for ICoFR as well as the full range of other areas including product quality, safety, security, customer service, cost containment, etc. The focus in this system is determining the level and amount of management attention that residual risk situations warrant. This approach is consistent with proposals made in the Australian public sector in the mid 1990s.

4. MANDATORY ICoFR ASSESSMENT METHOD(S)

Countries that decide to implement mandatory management reporting on ICoFR must decide early on whether they will 1) allow management broad flexibility when deciding how to go about the task of assessing and reporting ICoFR, 2) prescribe specifically how management should do the task, or 3) settle somewhere in the middle.

In the U.S. over the first two rounds of SOX reporting PCAOB AS2 prescribed in considerable detail how auditors should approach the task of assessing and reporting on ICoFR. No similar guidance existed for management at the time so management, quite logically, used the assessment criteria their auditors must use per the PCAOB. The SEC announced in May of 2006 that they plan on issuing guidance for management sometime in the future and have started the process of soliciting feedback on what that guidance should contain.

The current PCAOB AS ICoFR assessment guidance generally prescribes a bottom-up "process/control testing centric" assessment approach for the majority of the assessment work required. Auditors have used this type of approach to assessing ICoFR for many decades. No specific guidance is provided for auditors in AS2 on how to assess whether a client has, in fact, done their ICoFR assessment against the control criteria prescribed in COSO 1992 or any other framework they might be reporting against. When using a process-centric assessment approach a company usually will link specific accounts and financial statement notes to one or more business processes that support them. These business processes are then documented, evaluated and controls tested to arrive at a conclusion on any deficiencies noted in the process. Risks to the process objectives may, or may not, be identified, evaluated and prioritized. Residual risk status, specifically current process error rate/reliability, is not generally identified. The conclusions on the processes that support specific account balances are used to support management and auditor conclusions that the controls that support reliable financial statements and sub-components are, by extension, effective or ineffective. Because of the current guidance in AS2 IMA research has revealed that many companies did not complete entity level risk-based assessments on the macro level objective of reliable financial statements with the full agreement of their external auditors. To support claims that ICoFR assessments were done in accordance with COSO some companies did high level, "control criteria centric" assessments in addition to very detailed "process-centric" work. Based on the September 2006 IMA SOX research study not all audit firms required that companies specifically and visibly evaluate their ICoFR controls against the criteria in COSO 1992 to support claims the assessment was done in accordance with COSO.

In countries that require external auditors separately opine on control effectiveness or opine on the approach used by management **it is important that regulators provide at least broad guidance on the ICoFR assessment method(s) they consider appropriate for management to complete assessments of ICoFR to ensure some level of repeatability.** If no specific ICoFR assessment methods are prescribed by regulators, the goal of management and/or auditors reaching reasonably consistent opinions on control effectiveness will not likely be achieved nor will the goal of the information being consistent across companies.

5. MANDATORY USE OF ONE OR MORE CONTROL FRAMEWORK/CRITERIA

Current U.S. regulations require that management use a control framework that the SEC has indicated is "suitable". The SEC has stipulated four specific criteria a framework must meet to qualify as "suitable" (see page v in the Authority & Acknowledgements section). COSO 1992, the Canadian CoCo and/or assessment guidance, and the U.K. Cadbury/Turnbull guidance are specifically referenced as frameworks the SEC believes meet their suitability criteria. In the case of the Canadian and U.K. frameworks, it isn't clear if the SEC is approving the original control frameworks that most closely parallel the COSO 1992 integrated framework, or subsequent guidance that was issued in both countries on how to go about the task of assessing and reporting on ICoFR using those frameworks. What is clear is that the ICoFR assessment guidance issued in Canada in 1999 and the U.K. by the Turnbull Commission is not consistent with the much more granular ICoFR assessment methodology detailed in PCAOB AS2.

The September 2006 IMA SOX research study and a Financial Executives Research Foundation study on control deficiency reporting issued in 2005 raise considerable doubt that any control framework in the world, on its own, is capable of actually meeting current SEC suitability criteria defining a legally "fit for purpose" controls and assessment framework. The two most challenging criteria to test or "prove" are a) the

repeatability criterion – the need to produce reasonably consistent quantitative and qualitative conclusions on control effectiveness, and b) the completeness criterion - the ability to comprehensively integrate all control aspects necessary to reach a fully supported conclusion on ICoFR including fraud risk, IT controls, etc.

The September 2006 IMA SOX research study also indicates that a large percentage of companies use the COBIT framework for assessing the IT general controls – as previously indicated, this finding was even more definitively collaborated by an ISACA survey with over 700 respondents in April, 2006. A majority of respondents in both surveys indicated that they are not using COSO 1992 for the IT or fraud related dimensions of assessing ICoFR. The COBIT assessment framework is not currently listed as an SEC approved ICoFR assessment framework. Some companies have done little to support that they have actually evaluated their micro and macro level ICoFR control against COSO criteria particularly with respect to financial statement note disclosures. The IMA is currently considering conducting a new empirically-based research study, using statistically validated experimental design techniques", to evaluate whether current rules are actually resulting in reasonably consistent quantitative and qualitative conclusions on ICoFR.

We recommend that "unless and until" existing control frameworks are tested in some reasonable manner to determine whether they are, in fact, capable of meeting all four SEC listed suitability criteria (particularly repeatability and completeness), U.S. regulators either eliminate or significantly modify the specific language in the Final Rule. We also believe that a statement from management indicating how they have approached the task of assessing and reporting on ICoFR, including a description of any reference criteria used including frameworks like COSO 1992, COSO linked frameworks including their source, COBIT, AICPA anti-fraud criteria, etc. would be more useful and valid than prescribing that management report against a single framework. Perhaps we would modify this recommendation if some efforts were made to "harmonize" existing and evolving global frameworks, but this clearly is a longer-term initiative.

5. IMPLICATIONS FOR REGULATORS OUTSIDE THE U.S.

We believe that the core intent of SOX remains valid and that it will eventually be validated by empirical research. We also believe however that the current U.S. regulations to implement SOX are in need to significant changes. Regulators interested in protecting the integrity of the capital markets should carefully consider the implications of the issues raised in this paper.

ATTACHMENT 1
TOP-DOWN/RISK-BASED ICOFR ASSESSMENTS
STEP BY STEP

Step 1 — The Really Big Picture

Develop one or more entity level ICoFR assurance contexts. Start with the assurance context of "Ensure reliable auditor certified financial statements" at the consolidated level. Add additional macro assurance contexts for each subsidiary/unit with a separate financial statement close process. **Smaller companies** with a single general ledger will only need to complete one entity/top-level risk/control assessment.

Step 2 — A Risk-Based Approach to The Really Big Picture

Complete risk and control assessments on the top-level assurance contexts, following the broad steps outlined in this paper. Ensure that auditor mandated accounting adjustments and management detected errors discovered after release of public disclosures are included as part of residual risk status indicator data. Take particular care to ensure that macro level fraud related risks that have proven to be plausible, including senior management override of controls and other major risks that led to the enactment of legislation like SOX in the U.S. are addressed at this stage. This paper provides more details on how to complete macro level assessments including identification of risks, mitigating controls and residual risk status.

Step 3 — Create a Top-Down Universe of Assurance Contexts and "Risk Rate" Them

Expand the universe of assurance contexts to include the material account balances in public disclosures, material financial statement line item sub-components, and all financial statement note disclosures. Include assurance contexts related to IT security and a macro level anti-fraud objective. "Risk-rate" each of the assurance contexts using the type of criteria outlined in this paper in Section 3.3 The goal is to demonstrate that a reasonable effort was made to determine which assurance contexts that support the macro level objectives of reliable auditor certified financial statements warrant additional investment of time and money formally assessing risks and controls and, most importantly, residual risk status. These ratings should be updated periodically to reflect any new information.

Step 4 — Getting More Granular

For assurance contexts that have risk ratings above management determined, auditor determined, or regulator determined assessment granularity or materiality thresholds, increase the amount of risk and control design analysis and controls confirmation and independent testing work in proportion to their overall risk score. Put particular emphasis on identifying significant risks and evaluating the effectiveness of the company's current mitigation strategy in terms of the current process error rate as evidenced by management detected and auditor detected errors in the accounts and notes to the financial statements.

Step 5 — Decide on Update Frequency or Follow Applicable Laws re Update Frequency

Your security regulator may stipulate the frequency that the ICoFR assessment process needs to be updated. Current SOX regulations pursuant to Section 302 in the U.S. call for quarterly reports on any significant deficiencies or material weaknesses to audit committees and external auditors, reports to regulators on resolution of significant deficiencies and material weaknesses and reports to regulators of any "significant changes in internal controls or other factors that could subsequently affect internal controls". What constitutes a significant change in internal controls has not been defined by U.S. regulators and is open to reasonable interpretation currently. In cases where there are no specific regulator mandated rules, update frequency can be determined based on a periodic update of the assurance contexts risk scores.

Step 6 — Periodically Reassess the ICoFR Process Reliability

Carefully monitor the "predictive ability" of your ICoFR assessment system. When material errors in accounts or financial statement notes are detected that were not predicted by the company's risk and control assessment system, a reassessment of the approach used to assess and report on ICoFR should be undertaken to increase it's predictive reliability.

ATTACHMENT 2
EXAMPLE OF A "RISK SOURCE" FRAMEWORK TO HELP IDENTIFY RISKS

Commercial/Legal
Is the entity or objective threatened by contractual issues or relationships or the absence of contracts or by legal or regulatory requirements?

Competition
Is the entity or objective threatened by the actions of competitors including illegal, unethical, collusive and/or strategic actions of competitors?

Control Design
Is the entity or objective threatened by structural deficiencies in the overall approach to control used by the organization? (i.e. the macro control design)

Customers
Is the entity or objective threatened by the actions of customers outside the normal course of business?

Employees
Is the entity or objective threatened the actions of employees involved in organized or unorganized collective actions? (Note: this risk source covers collective actions as opposed to the risk source covered in the Human Behaviour category)

Environmental Liability
Is the entity or objective threatened by liabilities or hazards from environmental events, exposures or situations?

Equipment/Technology
Is the entity or objective threatened by failures or deficiencies in equipment and/or technology including computer hardware and software?

Finance/Economic
Is the entity or objective threatened by general economic or financial conditions, lack of funds trends either positive or negative?

Fraud/Corruption
Is the entity or objective threatened by fraudulent acts of employees, suppliers, customers or outside parties including organized crime schemes?

Human Behaviour
Is the entity or objective threatened by the behaviours of the people necessary to support the objective including employees, suppliers, agents, outsourcer activities etc.? (e.g. forgetfulness, indifference, defiance, etc.)

Missing Objectives
Is the entity or objective threatened by the absence of any key supporting objectives necessary for the long-term success of the entity or to support a specific objective?

Natural Events
Is the entity or objective threatened by natural events such as lightning, floods, fire, ice storms, wildlife, temperature variations, etc?

Political Influences
Is the entity or objective threatened by possible political or regulatory intervention and/or legislation?

Product/Service Liability
Is the entity or objective threatened by liabilities from the products or services provided by the organization or acquired by the organization from others including any outsourcing or sub-contract relationships?

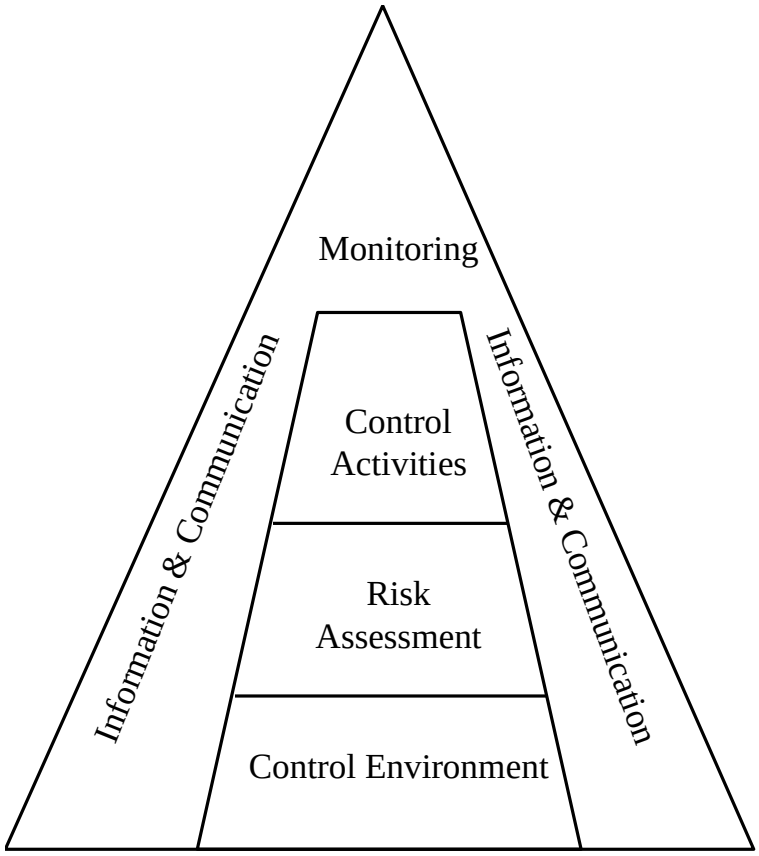
Public Perception
Is the entity or objective threatened the consequences that can flow from public reaction to corporate activities including media reports or other information they obtain about the organization's activities?

Suppliers
Is the entity or objective threatened by the actions of suppliers including the goods and/or services they provide?

It is important to note that this is not an exhaustive trigger list. However, it has proven effective as a tool to assist users in expanding their frame of reference when completing risk assessments.

ATTACHMENT 3
COSO 1992 CONTROL CATEGORIES

The Model



The Definition

Internal control is a process, effected by an entity's board of directors, management and other personnel, designated to provide reasonable assurance regarding the achievement of objectives in the following categories:

- *Effectiveness and efficiency of operations.*
- *Reliability of financial reporting.*
- *Compliance with applicable laws and regulations.*

The control environment provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It services as the foundation for the other components. Within this environment, management assesses risks to the achievement of specified objectives. Control activities are implemented to help ensure that management directives to address the risks are carried out. Meanwhile, relevant information is captured and communicated throughout the organization. The entire process is monitored and modified as conditions warrant.

ATTACHMENT 4
AN INTERPRETATION OF COSO 1992

(Not Evaluated by COSO)

CE CONTROL ENVIRONMENT

CE 1. Integrity and Ethical Values

CE 1.1 Definition and Communication of Corporate Conduct Values and Standards

The organization has communicated its values and standards to employees, suppliers, customers and other relevant stakeholders. There is a process to update and communicate these standards and related training regularly.

CE 2. Commitment to Competence

CE 2.1 Job Descriptions

Employees know through job descriptions or other documentation the specific business/quality objectives their daily work supports.

CE 2.2 Knowledge/Skills Gap Identification and Resolution Tools/Processes

There are processes in place to define the knowledge levels and skills necessary to successfully meet job responsibilities; inventory the knowledge and skills of the people doing the work or being considered for job assignments, and frameworks or processes to close any knowledge/skill gaps identified.

CE 2.3 Other Training/Education Methods

There are any other processes or activities which increase the assurance that people have the necessary knowledge and skill.

CE 2.4 Reference Aids

There are reference aids or resources available which employees can refer to assist them in fulfilling their job responsibilities.

CE 3. Board of Directors or Audit Committee

CE 3.1 Officer/Board Level Review

Senior management and/or the board of directors ask for information and reports on specific business/quality objectives and/or the adequacy of the systems and processes that support the achievement of those objectives.

CE 3.2 External Audits

Personnel external to the organization are used to assess and report on the organization's public disclosures particularly those related to the organization's financial status.

CE 3.3 Specialist Reviews & Audits

The organization engages specialists from time to time to examine and report on the way the organization is managing specific issues or areas of business activity. These reviews can relate to any facet of an organization's activities including such things as customer service, product quality, cost minimization, safety, fraud prevention, regulatory compliance, computer security, derivatives trading operations, and others.

CE 4. Management's Philosophy and Operating Style

CE 4.1 Strategic Business Analysis

The organization periodically analyzes the current level of achievement relative to what the organization believes should or must be accomplished.

CE 4.2 Short, Medium and Long Range Planning

The organization plans for the immediate future, usually covering the next year, the medium term often viewed as a two to five year time horizon, and the longer term which may stretch out many decades.

CE 4.3 Communication of Business/Quality Objectives
End result business/quality objectives are communicated to all the people that must support the achievement of those objectives.

CE 5. Organizational Structure
CE 5.1 Organization Design
The design of the organization and sub units assist in clarifying who is responsible and/or accountable for specific business/quality objectives.
CE 5.2 Self-Assessment Forums & Tools
A process exists for people individually or collectively to take time to consider whether their current knowledge levels, skill sets, and resource levels are adequate to achieve the organization's business/quality objectives.

CE 6. Assignment of Authority and Responsibility
CE 6.1 Authority Grids/Structures & Procedures
The organization has formalized criteria that specify the level of management, up to and including the board of directors that must review and approve decisions taken or being considered by employees and management in the business units. Authority grids may exist which relate to capital spending, hiring of senior executives, risk exposure positions related to derivatives or foreign currency movement, decisions to undertake new lines of business, geographic expansion plans, access to computer systems and files, and many others.

CE 7. Human Resource Policies and Practices
CE 7.1 Performance Evaluation System
There are clear linkages between publicized business/quality objectives and the employee performance evaluation system(s) in use.
CE 7.2 Coaching/Training Activities & Processes
There are processes in place to close knowledge or skill gaps through coaching and/or other forms of training activities. These can be informal methods such as on the job coaching and feedback, or involve more formalized training in classroom or workshop environments.
CE 7.3 Hiring and Selection Procedures
The hiring and selection process formally considers the knowledge and skill attributes of candidates and attempt to hire or select personnel that have knowledge and skill profiles as close to the desired knowledge and skill profile as is possible. Or alternatively, if knowledge and skill mismatches are accepted consciously, are steps taken to mitigate the risks that may result.
CE 7.4 Performance Evaluation
The performance evaluation process in use attempt to identify and correct performance related problems which are being caused by knowledge and/or skills gaps.
CE 7.5 Motivation/Reward/Punishment Mechanisms
There are personal consequences related to the accomplishment or non-accomplishment of specific business/quality objectives.
CE 7.6 Firing and Discipline Practices
There are negative consequences attached to lack of commitment to business/quality objectives up to and including firing of those responsible for supporting the achievement of those objectives
CE 7.7 Career Planning Processes
The organization has formalized processes to identify the developmental steps necessary to ensure employees are acquiring knowledge, skill and experience necessary to fill positions that may open up or emerge in the organization in the future.
CE 7.8 Promotion Practices
There is linkage between the organization's stated objectives and the performance of those that are being promoted or demoted.
CE 7.9 Reward Systems – Monetary
There is visible linkage between the accomplishment of specific objectives and the monetary rewards provided by the organization.
CE 7.10 Reward Systems - Non-Monetary
There are any non-monetary techniques or methods that provide positive consequences for achievement of business/quality objectives, or negative consequences for the non-achievement of the objectives. (e.g. employee or team awards, special recognition, plaques, posters showing units that are not meeting targets, etc.)

RA RISK ASSESSMENT

RA 1. Entity-Wide Objectives

RA 1.1 Definition of Corporate Mission & Vision

The organization has defined its primary reason for existence. The organization has a documented mission and/or vision statement

RA 1.2 Risk Assessment Processes - Macro Level

There are mechanisms or forums to identify, consider and analyze the significant risks which may threaten the achievement of the organization's business/quality objectives including risks related to inadequate human and/or monetary resources.

RA 1.3 Definition of Entity Wide Objectives

The organization has defined the business/quality objectives that it needs to accomplish. They include objectives related to financial reporting, asset safeguarding, customer service, product quality, cost control, revenue generation, fraud prevention, reliable business information, compliance.

RA 1.4 Risk Assessment Processes - Micro Level

There are any mechanisms or processes in place to analyze specific risks or threats which may result in the non-achievement of business/quality objectives of specific departments, business units or other part of the entity including risks caused by inadequate or inappropriate human, monetary or other resources.

RA 2. Activity-Level Objectives

RA 2.1 Definition of Unit Level Objectives

End result business/quality objectives defined for each business unit or team. These are linked to the entity wide objectives. There is a process to check that unit and activity level objectives support corporate level objectives.

RA 2.2 Definition of Activity Level Objectives

End result business/quality objectives are clearly defined and linked to all activities being carried out in the business units. People know what they are expected to do, and more importantly, why they are doing these activities.

RA 2.3 Control & Risk Self-Assessment

Work units or groups of employees with responsibility for specific objectives periodically take time to develop or clarify objectives, formally analyze the risks or threats to their objectives, and assess the ability of the controls in use or place to mitigate these threats.

RA 3. Risks

RA 3.1 Disaster Recovery/Contingency Planning

The organization has mechanisms or processes in place to anticipate and consider the possibility of significant negative and/or positive events and develop plans to deal with these situations.

RA 3.2 Other Planning & Risk Assessment Processes

There are any other processes or activities that relate to the analysis of the past, consideration of threats and opportunities that may occur in the future, and establishment of plans to achieve business/quality objectives.

RA 4. Managing Change

RA 4.1 Systems Development Methodologies

The organization uses some form of structured development method when designing or reengineering business systems products or processes that considers possible threats and obstacles to the achievement of objectives.

CA CONTROL ACTIVITIES

CA 1.1 Direct Controls Related to Business Systems

There are specific direct controls built in to business systems to ensure the desired results are achieved. (Note: these tend to be the type of controls auditors have historically concentrated on when evaluating control systems).

CA 1.2 Physical Safeguarding Mechanisms

There are controls which protect the organization's assets through direct measures such as locks on doors, bars on windows, use of safes to secure valuables, fences around the perimeter of a plant, armed guards protecting a work site, and other similar techniques.

CA 1.3 Reconciliations/Comparisons/Edits
There are traditional control techniques such as reconciling bank accounts, comparisons of subledger totals to control accounts, system edits, etc. that are relevant to the achievement of the objective.
CA 1.4 Validity/Existence Tests
There are mechanisms to validate the existence of assets. Fairly common examples include physical inventory counts to determine that quantities and descriptions of goods and/or supplies on hand are accurate, fixed asset inventories to validate the existence of items represented in the accounts, and other similar processes.
CA 1.5 Restricted Access
Data in manual files or computer stored records is protected from unauthorized access through systems based or manual techniques.
CA 1.6 Form/Equipment Design
The design of manual business forms, computer input screens, or equipment such as cash registers or computer input terminals assist to reduce the probability of errors.
CA 1.7 Segregation of Duties
Tasks or processes segregated to reduce the risk of accidental errors and/or fraud.
CA 1.8 Code of Accounts Structure
The design of the general ledger or subledger account codes assists in minimizing errors and allow for effective data capture and reporting.
CA 1.9 Other Direct Control Methods, Procedures, or Things
There are any other methods, procedures or things that have a direct impact on ensuring the achievement of business/quality objectives.

IC INFORMATION AND COMMUNICATION

IC 1. Information

IC 1.1 Performance Contracts/Evaluation Criteria
Are performance contracts or other forms of employee evaluation criteria linked to specific business/quality objectives. (i.e. is performance evaluation linked to specific end result business/quality objectives.)
IC 1.2 Budgeting/Forecasting Processing
The budget and forecasting process link the achievement of objectives to specific business units and/or individuals.
IC 1.3 Written Accountability Acknowledgements
Employees have been asked to formally acknowledge in some way that they accept responsibility for one or more business/quality objectives.
IC 1.4 Self-Assessment/Risk Acceptance Processes
Work units engage in self-assessment processes which assist in clarifying and/or reinforcing ownership of business/quality objectives.
IC 1.5 Continuous Improvement & Analysis Tools
The organization and/or sub units use any formalized techniques to continuously review and improve work methods and processes. (e.g. total quality management tools, recognized quality systems such as Malcolm Baldrige, European Quality Model, ISO 9000 series of standards, etc).
IC 1.6 ISO Review/Regulator Inspections
The organization periodically measures its business methods and frameworks against known control or quality criteria such as: the ISO 9000 and 14000 series of standards; quality frameworks including the Malcolm Baldrige system, European Quality Foundation model, derivatives of the Baldrige systems; a disclosed control model such as COSO, COCO, the MCS Control Assurance & Risk Design Model, or regulatory criteria related to specific industries or areas of business activity.
IC 1.7 Other Process Oversight Activities
There are any other methods, procedures or other activities which are designed to assess the appropriateness of the control and risk management frameworks in place or in use in the organization.

IC 2. Communication

IC 2.1 Employee Surveys
Employees are periodically surveyed to determine their views and attitudes to the organization. Employees view the organization as a good place to work. Employees believe that the organization treats them fairly and with respect.

IC 2.2 Employee Focus Groups

The organization periodically assembles groups of employees to discuss and obtain feedback on issues important to the success of the organization. The organization works to create shared visions of what is important, rather than imposing one or more senior manager's vision of what the organization stands for, and the direction it is taking to succeed.

IC 2.3 Employee Question/Answer Vehicles

Management at all levels provides opportunities for employees to ask questions regarding the organization's direction, treatment of employees, ethical values, and other areas of employee concern or interest.

IC 2.4 Management Communication Processes

Management personnel at all levels are encouraged and trained to effectively communicate with employees in their business units. There are mechanisms in place to identify managers that are weak in this skill area. The organization have vehicles such as e-mail, newsletters, communication hotlines, etc. that provide mechanisms which encourage frank and candid communication with staff.

M MONITORING

M 1. Ongoing Monitoring

M 1.1 Manager/Officer Monitoring/Supervision

Managers at all levels periodically assess the areas they are responsible for to determine if the current control and risk management designs in place are resulting in an acceptable level of residual risk. Managers and officers can demonstrate that the controls in use or place are conscious selections.

M 1.2 Results & Status Reports/Reviews

There are processes or other mechanisms in use or place which report on or examine the achievement status of a particular objective or objectives. A common example is the review of the monthly or quarterly financial results by senior management or the board against targets. Other examples include a safety review meeting, environmental status review, customer service level reports, and many others.

M 1.3 Analysis: Statistical/Financial/Competitive

There are analysis processes in place or use that analyze current achievement levels against relevant benchmarks or planned achievement levels.

M 1.4 Benchmarking Tools/Processes

The organization benchmark current achievement levels against the levels or outputs achieved by others. Common examples include benchmarking the cost to produce a defined product or service relative to that of others, comparing service levels provided relative to competitors, performance of a fund manager compared to that of other fund managers, and many other applications.

M 1.5 Employee/Supervisor Observation

Employees and/or supervisors observe directly the current status of achievement related to one or more business/quality objectives. This can include a service supervisor observing the length of a line-up for bank services, a construction worker assessing if a pipeline is being built to the required specifications, an employee spotting a flawed product being loaded for shipment, etc.

M 2. Separate Evaluations

M 2.1 Self-Assessment Quality Assurance Reviews

The organization utilizes self-assessment processes to examine and report on all or part of the operation, and the self-assessment reports are subjected to some form of quality assurance review to ensure that they are producing reliable information.

M 2.2 Internal Audits

Internal audit personnel periodically review specified topics or business areas to analyze whether the controls selected are cost effective and resulting in a level of assurance and residual risk that is acceptable to the work unit, senior management and the board of directors. (e.g. internal auditors, safety auditors, environmental auditors, quality auditors, etc.)

M 3. Reporting Deficiencies

M 3.1 Self-Assessments/Direct Report Audits

There are self-assessment activities which include specific consideration of how well an objective is, or is not being achieved. There are audits performed by people not responsible for the activity or objective which examine and consider the current achievement status relative to some desired or required status.

M 3.2 Customer Survey Tools/Processes

There are activities and processes that seek information and feedback from customers in relation to a business/quality objective or objectives. These processes may be very sophisticated and intensive, or as simple as a customer complaint hotline.

M 3.3 Automated Monitoring/Reporting Mechanisms & Reports

There are any measurement activities undertaken by computers or machines which result in action occurring if the mechanism indicates situations outside of acceptable tolerance.

M 3.4 Integrity Concerns Reporting Mechanisms

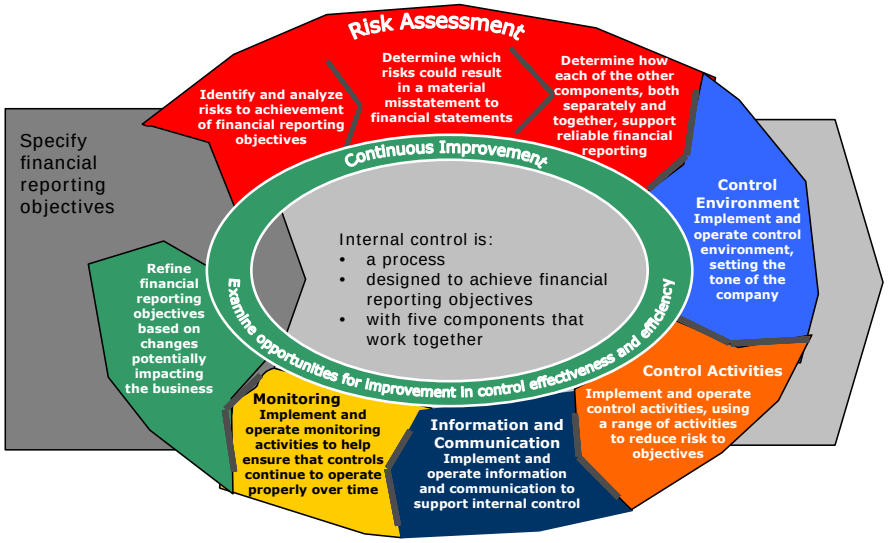
There are reporting options in place that allow people to report situations which are, or may be, violations of corporate ethical standards or societal objectives without fear of reprisal. Integrity concerns relate to areas such as employee or corporate honesty, individual or corporate compliance with the law, treatment of people, and other similar situations. These are also referred to as hotlines, or whistleblowing options.

M 3.5 Other Indicator/Measurement Controls

There are other methods, procedures or other things that assist in determining how well or how badly a specified business/quality objective is, or is not being achieved.

ATTACHMENT 5
COSO 2006 SMALLER PUBLIC COMPANY CONTROL CRITERIA

Navigating Internal Control Over Financial Reporting – Guidance for Smaller Public Companies



RISK ASSESSMENT

8. Identify financial reporting objectives - Complies with GAAP, supports information disclosures, reflects company activities, are supported by relevant financial statement assertions and considers materiality…
9. Identify and analyze financial reporting risks- Includes business processes, personnel and information technology, involves appropriate levels of management, considers both internal and external factors, estimates likelihood and impact, and triggers reassessment …
10. Identify and assess the risk of fraud as it affects the company - Considers incentives and pressures, risk factors, and establishes responsibilities and accountability …

CONTROL ENVIRONMENT

1. Integrity and ethical values are developed and understood - Articulates values, monitors adherence, addresses deviations …
2. Board of directors understand and exercise oversight - Defines authorities, operates independently, monitors risk, retains financial reporting expertise, oversees quality and reliability and oversees audit activities …
3. Management philosophy and operating style support internal control - Sets the tone, influences attitudes towards accounting principles and estimates and articulates objectives …
4. Organizational structure supports internal control - Establishes lines of financial reporting and establishes structure …
5. Financial reporting competencies are retained - Identifies competencies, retains individuals and evaluate competencies …
6. Authority and responsibility are assigned - Defines responsibilities and limits authority …
7. Human resource policies and practices facilitate internal control - Establishes human resource practices, recruits and retains, adequately trains, and evaluates performance and compensates …

CONTROL ACTIVITIES

11. Controls activities integrate with risk assessment - Mitigate risks, considers all significant points of entry into the company's G/L and information technology …
12. Controls activities are selected and developed - Considers range of activities, includes preventive and detective controls, segregates duties, and considers cost vs. benefit …
13. Policies are established and communicated and result in management directives being carried out - Integrates into business Processes, establishes responsibility and authority, occurs on a timely basis, thoughtfully implements, investigates exceptions, and periodically reassesses …
14. Information technology controls are designed and implemented - Includes application controls, considers general computer operations, and includes end-user computing …

INFORMATION AND COMMUNICATION

15. Financial reporting information is identified, captured, used and distributed - Captures data, includes financial information, uses internal and external sources, includes operating information, and maintains quality …
16. Internal control information is identified, captured, used and distributed - Captures data, triggers resolution and update, and maintains quality …
17. Internal communication supports execution of internal control - Communicates with personnel and board, includes separate communication lines, and accesses information …
18. Matters affecting achievement objectives are communicated - Provides input and independently assesses …

MONITORING

19. Ongoing and/or separate evaluations enable management to determine function of internal control - Integrates with operations, provides objective assessment, uses knowledgeable personnel, considers feedback and adjust scope and frequency …
20. Internal control deficiencies are identified and communicated - Reports findings and deficiencies, and corrects on a timely basis …

Excerpt from COSO Internal Controls Over Financial Reporting – Guidance for Smaller Public Companies – Volume II Guidance

ATTACHMENT 6
CANADIAN CRITERIA OF CONTROL FRAMEWORK

September 1995

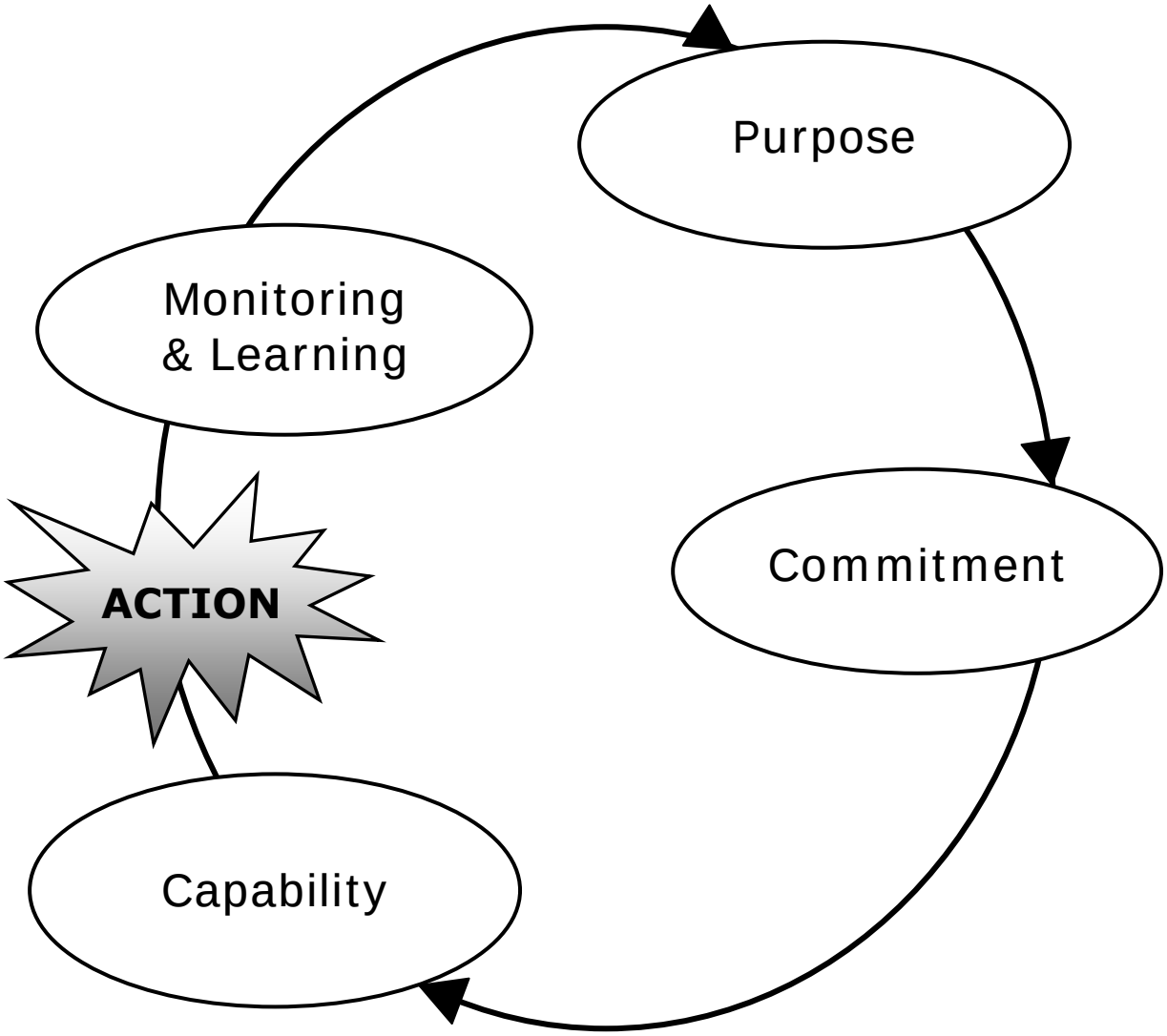


Exhibit B - The Criteria

PURPOSE

A1 Objectives should be established and communicated.

A2 The significant internal and external risks faced by an organization in the achievement of its objectives should be identified and assessed.

A3 Policies designed to support the achievement of an organization's objectives and the management of its risks should be established, communicated and practised so that people understand what is expected of them and the scope of their freedom to act.

A4 Plans to guide efforts in achieving the organization's objectives should be established and communicated.

A5 Objectives and related plans should include measurable performance targets and indicators.

COMMITMENT

B1 Shared ethical values, including integrity, should be established, communicated and practised throughout the organization.

B2 Human resource policies and practices should be consistent with an organization's ethical values and with the achievement of its objectives.

B3 Authority, responsibility and accountability should be clearly defined and consistent with an organization's objectives so that decisions and actions are taken by the appropriate people.

B4 An atmosphere of mutual trust should be fostered to support the flow of information between people and their effective performance toward achieving the organization's objectives.

CAPABILITY

C1 People should have the necessary knowledge, skills and tools to support the achievement of the organization's objectives.

C2 Communication processes support the organization's values and the achievement of its objectives.

C3 Sufficient and relevant information should be identified and communicated in a timely manner to enable people to perform their assigned responsibilities.

C4 The decisions and actions of different parts of the organization should be coordinated.

C5 Control activities should be designed as an integral part of the organization, taking into consideration its objectives, the risks to their achievement, and the inter-relatedness of control elements.

MONITORING AND LEARNING

D1 External and internal environments should be monitored to obtain information that may signal a need to re-evaluate the organization's objectives or control.

D2 Performance should be monitored against the targets and indicators identified in the organization's objectives and plans.

D3 The assumptions behind an organization's objectives and systems should be periodically challenged.

D4 Information needs and related information systems should be reassessed as objectives change or as reporting deficiencies are identified.

D5 Follow-up procedures should be established and performed to ensure appropriate change or action occurs.

D6 Management should periodically assess the effectiveness of control in its organization and communicate the results to those to whom it is accountable.

ATTACHMENT 7
CADBURY DECEMBER 1994 IN THE U.K.

1. Control environment

- A commitment by directors, management and employees to competence and integrity (e.g. leadership by example, employment criteria).
- Communication of ethical values and control consciousness to managers and employees (e.g. through written codes of conduct, formal standards of discipline, performance appraisal).
- An appropriate organisational structure within which business can be planned, executed, controlled and monitored to achieve the company's/group's objectives.
- Appropriate delegation of authority with accountability which has regard to acceptable levels of risk.
- A professional approach to financial reporting which complies with generally accepted accounting practice.

2. Identification and evaluation of risks and control objectives

- Identification of key business risks in a timely manner.
- Consideration of the likelihood of risks crystallising and the significance of the consequent financial impact on the business.
- Establishment of priorities for the allocation of resources available for control and the setting and communicating of clear control objectives.

3. Information and communication

- Performance indicators which allow management to monitor the key business and financial activities and risks, and the progress towards financial objectives, and to identify developments which require intervention (e.g. forecasts and budgets).
- Information systems which provide ongoing identification and capture of relevant, reliable and up-to-date financial and other information from internal and external sources (e.g. monthly management accounts, including earnings, cashflow and balance sheet reporting).
- Systems which communicate relevant information to the right people at the right frequency and time in a format which exposes significant variance s from the budgets and forecasts and allows prompt response.

4. Control procedures

- Procedures to ensure complete and accurate accounting for financial transactions.
- Appropriate authorisation limits for transactions that reasonably limit the company's/group's exposures.
- Procedures to ensure the reliability of data processing and information reports generated.
- Controls that limit exposure to loss of assets/records or to fraud (e.g. physical controls, segregation of duties).
- Routine and surprise checks which provide effective supervision of the control activities.
- Procedures to ensure compliance with laws and regulations that have significant financial implications.

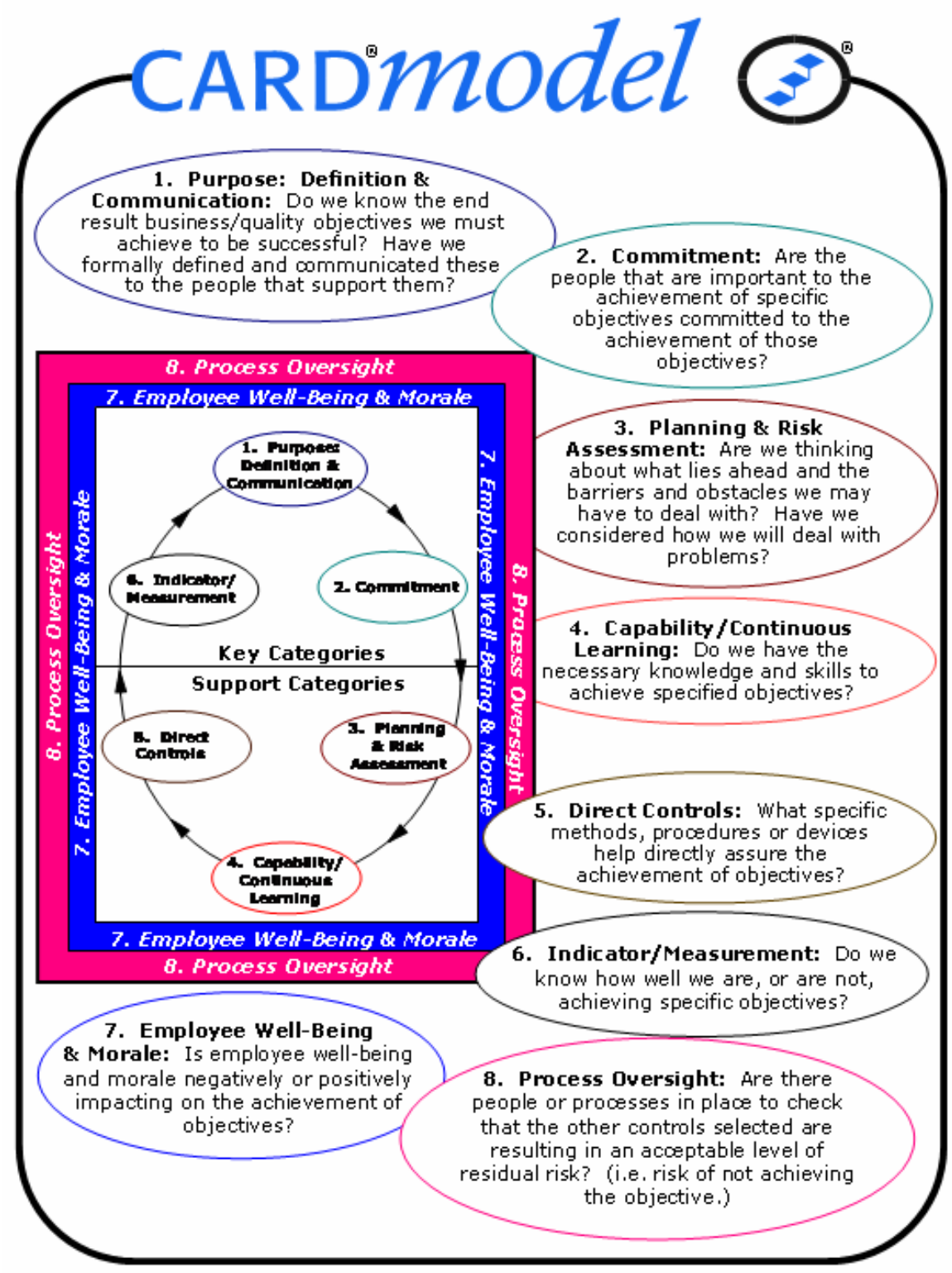
5. Monitoring and corrective action

- A monitoring process which provides reasonable assurance to the board that there are appropriate control procedures in place for all the company's/group's financially significant business activities and that these procedures are being followed (e.g. consideration by the board or board committee of reports from management, from an internal audit function or from independent accountants).
- Identification of change in the business and its environment which may require changes to the system of internal financial control.
- Formal procedures for reporting weaknesses and for ensuring appropriate corrective action.
- The provision of adequate support for public statements by the directors on internal control or internal financial control.

SOURCE: INTERNAL CONTROL AND FINANCIAL REPORTING: GUIDANCE FOR DIRECTORS OF LISTED COMPANIES REGISTERED IN THE U.K. - DECEMBER 1994.

Note: The more detailed framework that supports the structure shown above was included in the October 1993 exposure draft. The more detailed guidance was deleted in the final December 1994 report.

ATTACHMENT 8
CARD®*MODEL*: A COSO LINKED FRAMEWORK



CARD®menu

1. PURPOSE: DEFINITION & COMMUNICATION
1.1 Definition of Corporate Mission & Vision
1.2 Definition of Entity Wide Objectives
1.3 Definition of Unit Level Objectives
1.4 Definition of Activity Level Objectives
1.5 Communication of Business/Quality Objectives
1.6 Definition and Communication of Corporate Conduct Values and Standards

2. COMMITMENT
2.1 Accountability/Responsibility Mechanisms
2.1a Job Descriptions
2.1b Performance Contracts/Evaluation Criteria
2.1c Budgeting/Forecasting Processing
2.1d Written Accountability Acknowledgements
2.1e Other Accountability/Responsibility Mechanisms
2.2 Motivation/Reward/Punishment Mechanisms
2.2a Performance Evaluation System
2.2b Promotion Practices
2.2c Firing and Discipline Practices
2.2d Reward Systems - Monetary
2.2e Reward Systems - Non-Monetary
2.3 Organization Design
2.4 Self-Assessment/Risk Acceptance Processes
2.5 Officer/Board Level Review
2.6 Other Commitment Controls

3. PLANNING & RISK ASSESSMENT
3.1 Strategic Business Analysis
3.2 Short, Medium and Long Range Planning
3.3 Risk Assessment Processes - Macro Level
3.4 Risk Assessment Processes - Micro Level
3.5 Control & Risk Self-Assessment
3.6 Continuous Improvement & Analysis Tools
3.7 Systems Development Methodologies
3.8 Disaster Recovery/Contingency Planning
3.9 Other Planning & Risk Assessment Processes

4. CAPABILITY/CONTINUOUS LEARNING
4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes
4.2 Self-Assessment Forums & Tools
4.3 Coaching/Training Activities & Processes
4.4 Hiring and Selection Procedures
4.5 Performance Evaluation
4.6 Career Planning Processes
4.7 Firing Practices
4.8 Reference Aids
4.9 Other Training/Education Methods

5. DIRECT CONTROLS
5.1 Direct Controls Related to Business Systems
5.2 Physical Safeguarding Mechanisms
5.3 Reconciliations/Comparisons/Edits
5.4 Validity/Existence Tests
5.5 Restricted Access
5.6 Form/Equipment Design
5.7 Segregation of Duties
5.8 Code of Accounts Structure
5.9 Other Direct Control Methods, Procedures, or Things

6. INDICATOR/MEASUREMENT
6.1 Results & Status Reports/Reviews
6.2 Analysis: Statistical/Financial/Competitive
6.3 Self-Assessments/Direct Report Audits
6.4 Benchmarking Tools/Processes
6.5 Customer Survey Tools/Processes
6.6 Automated Monitoring/Reporting Mechanisms & Reports
6.7 Integrity Concerns Reporting Mechanisms
6.8 Employee/Supervisor Observation
6.9 Other Indicator/Measurement Controls

7. EMPLOYEE WELL-BEING & MORALE
7.1 Employee Surveys
7.2 Employee Focus Groups
7.3 Employee Question/Answer Vehicles
7.4 Management Communication Processes
7.5 Personal and Career Planning
7.6 Diversity Training/Recognition
7.7 Equity Analysis Processes
7.8 Measurement Tools/Processes
7.9 Other Well-Being/Morale Processes

8. PROCESS OVERSIGHT
8.1 Manager/Officer Monitoring/Supervision
8.2 Internal Audits
8.3 External Audits
8.4 Specialist Reviews & Audits
8.5 ISO Review/Regulator Inspections
8.6 Audit Committee/Board Oversight
8.7 Self-Assessment Quality Assurance Reviews
8.8 Authority Grids/Structures & Procedures
8.9 Other Process Oversight Activities

CARD®*menu* Trigger Questions

1.0 PURPOSE: DEFINITION & COMMUNICATION

Primary Category Definition: Do we know the end result business/quality objectives we must achieve to be successful? Have we formally defined and communicated these to the people that support them?

1.1 Definition of Corporate Mission & Vision

Has the organization defined its primary reason for existence? Does the organization have a documented mission and/or vision statement?

1.2 Definition of Entity Wide Objectives

Has the organization defined the business/quality objectives that it needs to accomplish? Do they include objectives related to customer service, product quality, cost control, revenue generation, fraud prevention, reliable business information, legal compliance, and others?

1.3 Definition of Unit Level Objectives

Are end result business/quality objectives defined for each business unit or team? Are these linked to the objectives defined in elements 1.1 and 1.2? Is there a process to check that unit and activity level objectives support corporate level objectives?

1.4 Definition of Activity Level Objectives

Are end result business/quality objectives clearly defined for, or linked to, all activities being carried out in the business units? Do people know what they are expected to do, and more importantly, why they are doing these activities?

1.5 Communication of Business/Quality Objectives

Have end result business/quality objectives been communicated to all the people that must support the achievement of those objectives? Do they understand what the objectives mean?

1.6 Definition and Communication of Corporate Conduct Values and Standards

Specifically in the area of objectives related to corporate conduct and ethics, has the organization communicated its values and standards to employees, suppliers, customers and other relevant stakeholders? Is there a process to update and communicate these standards regularly?

2.0 COMMITMENT

Primary Category Definition: Are the people that are important to the achievement of specific objectives committed to the achievement of those objectives?

2.1 Accountability/Responsibility Mechanisms

Has the organization or unit defined and assigned accountability for achieving business/quality objectives? (Note: it is important to distinguish between assigning accountability for completion of activities or processes versus defining accountability for end result business/quality objectives).

2.1a Job Descriptions
Do employees know through job descriptions or other documentation the specific business/quality objectives their daily work supports?

2.1b Performance Contracts/Evaluation Criteria
Are performance contracts or other forms of employee evaluation criteria linked to specific business/quality objectives? (i.e. is performance evaluation linked to specific end result business/quality objectives?)

2.1c Budgeting/Forecasting Processing
Does the budget and forecasting process link the achievement of objectives to specific business units and/or individuals?

2.1d Written Accountability Acknowledgements
Have employees been asked to formally acknowledge in some way that they accept responsibility for one or more business/quality objectives?

2.1e Other Accountability/Responsibility Mechanisms
Are there any other mechanisms which establish accountability for specific business/quality objectives?

2.2 Motivation/Reward/Punishment Mechanisms
Are there personal consequences related to the accomplishment or non-accomplishment of specific business/quality objectives?

2.2a Performance Evaluation System
Are there clear linkages between publicized business/quality objectives and the employee performance evaluation system(s) in use?

2.2b Promotion Practices
Is there linkage between the organization's stated objectives and the performance of those that are being promoted or demoted?

2.2c Firing and Discipline Practices
Are there negative consequences attached to lack of commitment to business/quality objectives up to and including firing of those responsible for supporting the achievement of those objectives?

2.2d Reward Systems - Monetary
Is there visible linkage between the accomplishment of specific objectives and the monetary rewards provided by the organization?

2.2e Reward Systems - Non-Monetary
Are there any non-monetary techniques or methods that provide positive consequences for achievement of business/quality objectives, or negative consequences for the non-achievement of the objectives? (e.g. employee or team awards, special recognition, plaques, posters showing units that are not meeting targets, etc.)

2.3 Organization Design
Does the design of the organization and sub units assist in clarifying who is responsible and/or accountable for specific business/quality objectives?

2.4 Self-Assessment/Risk Acceptance Processes
Do work units engage in self-assessment processes which assist in clarifying and/or reinforcing ownership of business/quality objectives?

2.5 Officer/Board Level Review
Does senior management and/or the board of directors ask for information and reports on specific business/quality objectives and/or the adequacy of the systems and processes that support the achievement of those objectives?

2.6 Other Commitment Controls
Are there any other mechanisms in use or place which increase the commitment of employees to achieve business/quality objectives?

3.0 PLANNING & RISK ASSESSMENT
Primary Category Definition: Are we thinking about what lies ahead and the barriers and obstacles we may have to deal with? Have we considered how we will deal with problems?

3.1 Strategic Business Analysis
Does the organization periodically analyze the current level of achievement relative to what the organization believes should or must be accomplished?

3.2 Short, Medium and Long Range Planning
Does the organization plan for the immediate future, usually covering the next year, the medium term often viewed as a two to five year time horizon, and the longer term which may stretch out many decades?

3.3 Risk Assessment Processes - Macro Level
Are there mechanisms or forums to identify, consider and analyze the significant risks which may threaten the achievement of the organization's business/quality objectives including risks related to inadequate human and/or monetary resources?

3.4 Risk Assessment Processes - Micro Level
Are there any mechanisms or processes in place to analyze specific risks or threats which may result in the non-achievement of business/quality objectives of specific departments, business units or other part of the entity including risks caused by inadequate or inappropriate human, monetary or other resources?

3.5 Control & Risk Self-Assessment
Do work units or groups of employees with responsibility for specific objectives periodically take time to develop or clarify objectives, formally analyze the risks or threats to their objectives, and assess the ability of the controls in use or place to mitigate these threats?

3.6 Continuous Improvement & Analysis Tools
Does the organization and/or sub units use any formalized techniques to continuously review and improve work methods and processes? (e.g. total quality management tools, recognized quality systems such as Malcolm Baldrige, European Quality Model, ISO 9000 series of standards, etc).

3.7 Systems Development Methodologies
Does the organization use some form of structured development method when designing or reengineering business systems products or processes that considers possible threats and obstacles to the achievement of objectives?

3.8 Disaster Recovery/Contingency Planning
Does the organization have mechanisms or processes in place to anticipate and consider the possibility of significant negative and/or positive events and develop plans to deal with these situations? Examples include disasters which impact on computer systems, executive kidnapping, terrorist attacks, major natural disasters, a hugely successful sales launch, demise of a competitor, new technology, negative or positive legislative developments, and others.

3.9 Other Planning & Risk Assessment Processes
Are there any other processes or activities that relate to the analysis of the past, consideration of threats and opportunities that may occur in the future, and establishment of plans to achieve business/quality objectives?

4.0 CAPABILITY/CONTINUOUS LEARNING
Primary Category Definition: Do we have the necessary knowledge and skills to achieve specified objectives?

4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes
Are there processes in place to define the knowledge levels and skills necessary to successfully meet job responsibilities; inventory the knowledge and skills of the people doing the work or being considered for job assignments, and frameworks or processes to close any knowledge/skill gaps identified?

4.2 Self-Assessment Forums & Tools
Does a process exist for people individually or collectively to take time to consider whether their current knowledge levels, skill sets, and resource levels are adequate to achieve the organization's business/quality objectives?

4.3 Coaching/Training Activities & Processes
Are there processes in place to close knowledge or skill gaps through coaching and/or other forms of training activities? These can be informal methods such as on the job coaching and feedback, or involve more formalized training in classroom or workshop environments.

4.4 Hiring and Selection Procedures
Does the hiring and selection process formally consider the knowledge and skill attributes of candidates and attempt to hire or select personnel that have knowledge and skill profiles as close to the desired knowledge and skill profile as is possible? Or alternatively, if knowledge and skill mismatches are accepted consciously, are steps taken to mitigate the risks that may result?

4.5 Performance Evaluation
Does the performance evaluation process in use attempt to identify and correct performance related problems which are being caused by knowledge and/or skills gaps?

4.6 Career Planning Processes
Does the organization have formalized processes to identify the developmental steps necessary to ensure employees are acquiring knowledge, skill and experience necessary to fill positions that may open up or emerge in the organization in the future?

4.7 Firing Practices
When serious efforts have been made to correct knowledge and skill gaps but the efforts have been unsuccessful, does the organization take steps to address capability and/or commitment problems through termination or job reassignment?

4.8 Reference Aids
Are there reference aids or resources available which employees can refer to assist them in fulfilling their job responsibilities?

4.9 Other Training/Education Methods
Are there any other processes or activities which increase the assurance that people have the necessary knowledge and skill?

5.0 DIRECT CONTROLS
Primary Category Definition: What specific methods, procedures or devices help directly assure the achievement of objectives?

5.1 Direct Controls Related to Business Systems
Are there specific direct controls built in to business systems to ensure the desired results are achieved? (Note: these tend to be the type of controls auditors have historically concentrated on when evaluating control systems).

5.2 Physical Safeguarding Mechanisms
Are there controls which protect the organization's assets through direct measures such as locks on doors, bars on windows, use of safes to secure valuables, fences around the perimeter of a plant, armed guards protecting a work site, and other similar techniques?

5.3 Reconciliations/Comparisons/Edits
Are there traditional control techniques such as reconciling bank accounts, comparisons of subledger totals to control accounts, system edits, etc. that are relevant to the achievement of the objective?

5.4 Validity/Existence Tests
Are there mechanisms to validate the existence of assets? Fairly common examples include physical inventory counts to determine that quantities and descriptions of goods and/or supplies on hand are accurate, fixed asset inventories to validate the existence of items represented in the accounts, and other similar processes.

5.5 Restricted Access
Is data in manual files or computer stored records protected from unauthorized access through systems based or manual techniques?

5.6 Form/Equipment Design
Does the design of manual business forms, computer input screens, or equipment such as cash registers or computer input terminals assist to reduce the probability of errors?

5.7 Segregation of Duties
Are tasks or processes segregated to reduce the risk of accidental errors and/or fraud?

5.8 Code of Accounts Structure
Does the design of the general ledger or subledger account codes assist in minimizing errors and allow for effective data capture and reporting?

5.9 Other Direct Control Methods, Procedures, or Things
Are there any other methods, procedures or things that have a direct impact on ensuring the achievement of business/quality objectives?

6.0 INDICATOR/MEASUREMENT
Primary Category Definition: Do we know how well we are, or are not, achieving specific objectives?

6.1 Results & Status Reports/Reviews
Are there processes or other mechanisms in use or place which report on or examine the achievement status of a particular objective or objectives? A common example is the review of the monthly or quarterly financial results by senior management or the board against targets. Other examples include a safety review meeting, environmental status review, customer service level reports, and many others.

6.2 Analysis: Statistical/Financial/Competitive
Are there analysis processes in place or use that analyze current achievement levels against relevant benchmarks or planned achievement levels?

6.3 Self-Assessments/Direct Report Audits
Are there any self-assessment activities which include specific consideration of how well an objective is, or is not being achieved? Are there audits performed by people not responsible for the activity or objective which examine and consider the current achievement status relative to some desired or required status?

6.4 Benchmarking Tools/Processes
Does the organization benchmark current achievement levels against the levels or outputs achieved by others? Common examples include benchmarking the cost to produce a defined product or service relative to that of others, comparing service levels provided relative to competitors, performance of a fund manager compared to that of other fund managers, and many other applications.

6.5 Customer Survey Tools/Processes
Are there activities and processes that seek information and feedback from customers in relation to a business/quality objective or objectives? These processes may be very sophisticated and intensive, or as simple as a customer complaint hotline.

6.6 Automated Monitoring/Reporting Mechanisms & Reports
Are there any measurement activities undertaken by computers or machines which result in action occurring if the mechanism indicates situations outside of acceptable tolerance?

6.7 Integrity Concerns Reporting Mechanisms

Are there reporting options in place that allow people to report situations which are, or may be, violations of corporate ethical standards or societal objectives without fear of reprisal? Integrity concerns relate to areas such as employee or corporate honesty, individual or corporate compliance with the law, treatment of people, and other similar situations. These are also referred to as hotlines, or whistleblowing options.

6.8 Employee/Supervisor Observation

Do employees and/or supervisors observe directly the current status of achievement related to one or more business/quality objectives? This can include a service supervisor observing the length of a line-up for bank services, a construction worker assessing if a pipeline is being built to the required specifications, an employee spotting a flawed product being loaded for shipment, etc.

6.9 Other Indicator/Measurement Controls

Are there any other methods, procedures or other things that assist in determining how well or how badly a specified business/quality objective is, or is not being achieved?

7.0 EMPLOYEE WELL-BEING & MORALE

Primary Category Definition: Is employee well-being and morale negatively or positively impacting on the achievement of objectives?

7.1 Employee Surveys

Are employees periodically surveyed to determine their views and attitudes to the organization? Do employees view the organization as a good or a bad place to work? Do they believe that the organization treats employees fairly and with respect?

7.2 Employee Focus Groups

Does the organization periodically assemble groups of employees to discuss and obtain feedback on issues important to the success of the organization? Does the organization work to create shared visions of what is important or does it impose one or more senior manager's vision of what the organization stands for, and the direction it is taking to succeed?

7.3 Employee Question/Answer Vehicles

Does management at all levels provide opportunities for employees to ask questions regarding the organization's direction, treatment of employees, ethical values, and other areas of employee concern or interest?

7.4 Management Communication Processes

Are management personnel at all levels encouraged and trained to effectively communicate with employees in their business units? Are there mechanisms in place to identify managers that are weak in this skill area? Does the organization have vehicles such as e-mail, newsletters, communication hotlines, etc. that provide mechanisms which encourage frank and candid communication with staff?

7.5 Personal and Career Planning

Are there mechanisms and processes in place which assist employees to think about their careers and consider ways to develop themselves and achieve their personal work related goals? Does the organization provide any management training or specialist assistance to help employees identify sources of help and guidance when they are having severe difficulties in their personal lives such as alcohol or drug dependencies, death of close family members, divorce, severe depression, etc?

7.6 Diversity Training/Recognition

Are managers and employees at all levels provided with awareness training, and if necessary, behaviour modification coaching, to ensure that they understand the value of diversity in the composition of work teams and organizations?

7.7 Equity Analysis Processes

Does the organization or work units periodically take time to self-assess or have other mechanisms to assess whether employees are being treated fairly in terms of pay, opportunities and other relevant areas?

7.8 Measurement Tools/Processes

Does the organization attempt to measure and track the state of morale in the organization and in the various business units that make it up to identify problems which may seriously impact on the organization's ability to achieve its objectives?

7.9 Other Well-Being/Morale Processes

Are there any other methods, procedures or other things which assist in measuring and improving employee morale?

8.0 PROCESS OVERSIGHT

Primary Category Definition: Are there people or processes in place to check that the other controls selected are resulting in an acceptable level of residual risk? (i.e. Risk of not achieving objectives).

8.1 Manager/Officer Monitoring/Supervision

Do managers at all levels periodically assess the areas they are responsible for to determine if the current control and risk management designs in place are resulting in an acceptable level of residual risk? Can managers and officers demonstrate that the controls in use or place are conscious selections, or are the controls in use a collection of activities that have evolved over the years without formal analysis occurring to evaluate the ongoing appropriateness of the controls and related risk levels?

8.2 Internal Audits

Do internal audit personnel periodically review specified topics or business areas to analyze whether the controls selected are cost effective and resulting in a level of assurance and residual risk that is acceptable to the work unit, senior management and the board of directors? (e.g. internal auditors, safety auditors, environmental auditors, quality auditors, etc.)

8.3 External Audits

Are personnel external to the organization used to assess and report on the organization's public disclosures particularly those related to the organization's financial status?

8.4 Specialist Reviews & Audits

Does the organization engage specialists from time to time to examine and report on the way the organization is managing specific issues or areas of business activity? These reviews can relate to any facet of an organization's activities including such things as customer service, product quality, cost minimization, safety, fraud prevention, regulatory compliance, computer security, derivatives trading operations, and others.

8.5 ISO Review/Regulator Inspections

Does the organization periodically measure its business methods and frameworks against known control or quality criteria such as: the ISO 9000 and 14000 series of standards; quality frameworks including the Malcolm Baldrige system, European Quality Foundation model, derivatives of the Baldrige systems; a disclosed control model such as COSO, COCO, the MCS Control Assurance & Risk Design Model, or regulatory criteria related to specific industries or areas of business activity?

8.6 Audit Committee/Board Oversight

Does the audit committee and the board of directors as a whole understand and fulfill their responsibility to oversee the adequacy of the control and risk management frameworks established by management? Has the board subjected the quality of their control governance oversight to a self-assessment process or an external review to check if they are measuring up to national and/or international governance best practices such as the Canadian standards for directors related to control governance? Is there evidence that the board of directors is asking for, and receiving, the quantity and quality of information on the status of control and risk necessary to fulfill their control governance responsibilities?

8.7 Self-Assessment Quality Assurance Reviews

If the organization utilizes self-assessment processes to examine and report on all or part of the operation, are the self-assessment reports subjected to some form of quality assurance review to ensure that they are producing reliable information?

8.8 Authority Grids/Structures & Procedures

Does the organization have formalized criteria that specifies the level of management, up to and including the board of directors that must review and approve decisions taken or being considered by employees and management in the business units? Authority grids may exist which relate to capital spending, hiring of senior executives, risk exposure positions related to derivatives or foreign currency movement, decisions to undertake new lines of business, geographic expansion plans, access to computer systems and files, and many others.

8.9 Other Process Oversight Activities

Are there any other methods, procedures or other activities which are designed to assess the appropriateness of the control and risk management frameworks in place or in use in the organization?

ATTACHMENT 9
COBIT 4.0 DOMAINS AND CONTROL PROCESS FOR ICOFR

COBIT 4.0 Control Objectives Relevant to Sarbanes-Oxley (SOX) SUMMARY TABLE

DOMAIN		PROCESS	Information							IT Resources			
			Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
Plan & Organise	PO1	Define a strategic IT plan	P	S						✓	✓	✓	✓
	PO2	Define the information architecture	S	P	S	P				✓	✓		
	PO3	Determine technological direction	P	P						✓		✓	
	PO4	Define the IT processes, organisation and relationships	P	P									✓
	PO5	Manage the IT investment	P	P					S	✓		✓	✓
	PO6	Communicate management aims and direction	P					S			✓		✓
	PO7	Manage IT human resources	P	P									✓
	PO8	Manage quality	P	P		S			S	✓	✓	✓	✓
	PO9	Assess and manage IT risks	S	S	P	P	P	S	S	✓	✓	✓	✓
	PO10	Manage projects	P	P						✓		✓	✓
Acquire & Implement	AI1	Identify automated solutions	P	S						✓		✓	
	AI2	Acquire and maintain application software	P	P		S			S	✓			
	AI3	Acquire and maintain technology infrastructure	S	P		S	S					✓	
	AI4	Enable operation and use	P	P		S	S	S	S	✓		✓	✓
	AI5	Procure IT resources	S	P				S		✓	✓	✓	✓
	AI6	Manage changes	P	P		P	P		S	✓	✓	✓	✓
	AI7	Install and accredit solutions and changes	P	S		S	S			✓	✓	✓	✓
Deliver & Support	DS1	Define and manage service levels	P	P	S	S	S	S	S	✓	✓	✓	✓
	DS2	Manage third-party services	P	P	S	S	S	S	S	✓	✓	✓	✓
	DS3	Manage performance and capacity	P	P			S			✓		✓	
	DS4	Ensure continuous service	P	S			P			✓	✓	✓	✓
	DS5	Ensure systems security			P	P	S	S	S	✓	✓	✓	✓
	DS6	Identify and allocate costs		P					P	✓	✓	✓	✓
	DS7	Educate and train users	P	S									✓
	DS8	Manage service desk and incidents	P	P						✓			✓
	DS9	Manage the configuration	P	S			S		S	✓	✓	✓	
	DS10	Manage problems	P	P			S			✓	✓	✓	✓
	DS11	Manage data				P			P		✓		
	DS12	Manage the physical environment				P	P					✓	
	DS13	Manage operations	P	P		S	S			✓	✓	✓	✓
Monitor & Evaluate	ME1	Monitor and evaluate IT performance	P	P	S	S	S	S	S	✓	✓	✓	✓
	ME2	Monitor and evaluate internal control	P	P	S	S	S	S	S	✓	✓	✓	✓
	ME3	Ensure regulatory compliance						P	S	✓	✓	✓	✓
	ME4	Provide IT governance	P	P	S	S	S	S	S	✓	✓	✓	✓

P Primary support in relation to SOX

S Secondary support in relation to SOX

PAISLEY CONSULTING *Business accountability solutions.*

ATTACHMENT 10
OPEN COMPLIANCE & ETHICS GROUP
FOUNDATION GUIDELINES OVERVIEW

C-Culture
- **C1-Ethical Culture**
  - **C1.1** Define Principles & Values
  - **C1.2** Enhance Ethical Climate & Mindsets
  - **C1.3** Foster Ethical Leadership
- **C2-Risk Culture**
  - **C2.1** Define Philosophy & Style
  - **C2.2** Enhance Risk Management Climate & Mindsets
- **C3-Governance Culture**
  - **C3.1** Define Governance Style & Approach
  - **C3.2** Enhance Governance Climate & Mindsets
- **C4-Workforce Culture**
  - **C4.1** Understand Workforce Management Philosophy & Style
  - **C4.2** Enhance Commitment to the Workforce & Competency
  - **C4.3** Enhance Workforce Satisfaction & Commitment

O-Organization / Personnel
- **O1-Leadership & Champions**
  - **O1.1** Define Leadership & Champion Responsibilities
  - **O1.2** Screen & Select Program Leadership & Champions
  - **O1.3** Enhance Champion Skills & Competencies
- **O2-Oversight Personnel**
  - **O2.1** Define Oversight Structure & Responsibilities
  - **O2.2** Screen & Select Oversight Personnel
  - **O2.3** Enhance Oversight Skills & Competencies
  - **O2.4** Assess Oversight Personnel & Team Performance
- **O3-Strategic Personnel**
  - **O3.1** Define Strategic Structure & Responsibilities
  - **O3.2** Screen & Select Strategic Personnel
  - **O3.3** Enhance Strategic Skills & Competencies
  - **O3.4** Assess Strategic Personnel & Team Performance
- **O4-Operational Personnel**
  - **O4.1** Define Operational Structure & Responsibilities
  - **O4.2** Screen & Select Operational Personnel
  - **O4.3** Enhance Operational Skills & Competencies
  - **O4.4** Assess Operational Personnel Performance

P-Process
- **PO-Plan & Organize**
- **PO1-Scope & Objectives**
  - **PO1.1** Define Scope
  - **PO1.2** Define Stakeholders
  - **PO1.3** Define Planning Methodology & Team
  - **PO1.4** Define / Review Organizational Objectives
  - **PO1.5** Define Program Objectives
- **PO2-Business Model & Context**
  - **PO2.1** Identify Key Organizational Entities, Units & Groups
  - **PO2.2** Identify Key Physical, Information and Technology Assets
  - **PO2.3** Identify Key Business Processes
  - **PO2.4** Identify Key Job Families, Positions, Roles & Assignments
- **PO3-Boundary Identification**
  - **PO3.1** Define Boundary Identification Methodology
  - **PO3.2** Identify Mandated Boundary
  - **PO3.3** Identify Voluntary Boundary
- **PO4-Event Identification**
  - **PO4.1** Define Event Identification Methodology
  - **PO4.2** Identify and Analyze Events
- **PO5-Risk Assessment**
  - **PO5.1** Define Risk Assessment Methodology
  - **PO5.2** Analyze Likelihood / Impact
  - **PO5.3** Define Priorities
- **PO6-Program Design & Strategy**
  - **PO6.1** Define Initiatives to Address Risks
  - **PO6.2** Define Initiatives to Address Opportunities & Values
  - **PO6.3** Select Initiatives, Controls & Accountability
  - **PO6.4** Define Crisis Responses
  - **PO6.5** Define Strategic Plan

PR-Prevent, Protect & Prepare
- **PR1-General Controls, Policies & Procedures**

PR1.1 Develop Controls, Policies & Procedures
PR1.2 Implement and Manage Controls, Policies & Procedures
PR1.3 Automate Controls, Policies & Procedures

PR2-Code Of Conduct
PR2.1 Develop Code of Conduct
PR2.2 Distribute and Manage Code of Conduct

PR3-Training & Education
PR3.1 Design / Develop Training
PR3.2 Implement and Manage Training

PR4-Workforce Management
PR4.1 Define Roles, Responsibilities & Duties
PR4.2 Screen & Select Workforce
PR4.3 Evaluate Performance & Promote Workforce
PR4.4 Compensate & Reward Workforce
PR4.5 Retire & Terminate Workforce

PR5-Physical Infrastructure
PR5.1 Design and Modify Physical Infrastructure

PR6-Risk Sharing & Insurance
PR6.1 Design and Implement Risk Sharing & Insurance

PR7-Preparedness & Practice
PR7.1 Design Preparedness Exercises
PR7.2 Conduct Preparedness Exercises

D-Detect, Monitor & Evaluate

M-Ongoing Monitoring

M1-Control Assurance & Audit
M1.1 Monitor Controls, Policies & Procedures
M1.2 Survey Employees and Other Stakeholders

M2-Hotline & Helpline
M2.1 Define Hotline/Helpline Approach
M2.2 Provide Hotline
M2.3 Provide Helpline

E-Periodic Evaluation

E1-Evaluation Planning & Reporting
E1.1 Define Evaluation Scope / Objectives
E1.2 Define Type of Evaluation
E1.3 Define Level of Assurance and Evaluation Team
E1.4 Define Privilege Status
E1.5 Develop Evaluation Plan
E1.6 Define and Communicate Evaluation Report Content

E2-Program Effectiveness Evaluation
E2.1 Perform Design Effectiveness (DE) Evaluation
E2.2 Perform Operating Effectiveness (OE) Evaluation

E3-Program Performance Evaluation
E3.1 Perform Program Efficiency (PE) Evaluation
E3.2 Perform Program Responsiveness (PR) Evaluation

R-Respond & Improve

R1-Incident, Issue & Case Management
R1.1 Process, Escalate & Manage Incidents
R1.2 Resolve Issues

R2-Special Investigation
R2.1 Determine Need/Scope of Investigation
R2.2 Create Investigation Team
R2.3 Plan Investigation
R2.4 Execute Investigation Plan
R2.5 Communicate Investigation/Follow-Up

R3-Crisis Response & Communication
R3.1 Execute Crisis and Emergency Response Plan

R4-Discipline & Disclosure
R4.1 Discharge Discipline
R4.2 Disclose Findings

R5-Remediation & Improvement
R5.1 Modify Program for Improvement

I-Information & Communication

I1-Information & Records Management
I1.1 Classify Data & Records
I1.2 Define Information Access
I1.6 Define Information Availability, Integrity & Recovery
I1.4 Define Information Management Monitoring
I1.3 Define Information Disposition
I1.6 Define Information Management & Records Awareness Program

I2-Communication
I2.1 Develop Communication Plan
I2.2 Deliver Communications

I3-Internal Reporting
I3.1 Develop Internal Reports

I4-External Reporting & Filings
I4.1 Develop Disclosure Systems and Forms
I4.2 Create and Manage Disclosures & Filings

T-Technology

T1-Technology
T1.1 Leverage Technology to Support Program

Excerpt from OCEG Foundation Guidelines Red Book, August 25, 2006

ATTACHMENT 11
SAMPLE COSO 1992
CONTROL CRITERIA CENTRIC ASSESSMENT

COSO 1992 Control Element	Degree Evidenced for Reliable Financial Reporting
1. CONTROL ENVIRONMENT	**Low** **High**
1.1 Integrity and Ethical Values	**1 2 3 4 5 6 7 8 9 10**
1.2 Commitment to Competence	**1 2 3 4 5 6 7 8 9 10**
1.3 Board of Directors/Audit Committee	**1 2 3 4 5 6 7 8 9 10**
1.4 Management Philosophy and Operating Style	**1 2 3 4 5 6 7 8 9 10**
1.5 Organization Structure	**1 2 3 4 5 6 7 8 9 10**
1.6 Assignment of Authority and Responsibility	**1 2 3 4 5 6 7 8 9 10**
1.7 Human Resource Policies and Practices	**1 2 3 4 5 6 7 8 9 10**
2. RISK ASSESSMENT	**Low** **High**
2.1 Entity-Wide Objectives	**1 2 3 4 5 6 7 8 9 10**
2.2 Activity-Level Objectives	**1 2 3 4 5 6 7 8 9 10**
2.3 Risk Identification	**1 2 3 4 5 6 7 8 9 10**
2.4 Change Management	**1 2 3 4 5 6 7 8 9 10**
3. CONTROL ACTIVITIES	**Low** **High**
3.1 Top Level Reviews	**1 2 3 4 5 6 7 8 9 10**
3.2 Direct Functional or Activity Management	**1 2 3 4 5 6 7 8 9 10**
3.3 Information Processing	**1 2 3 4 5 6 7 8 9 10**
3.4 Physical Controls	**1 2 3 4 5 6 7 8 9 10**
3.5 Performance Indicators	**1 2 3 4 5 6 7 8 9 10**
3.6 Segregation of Duties	**1 2 3 4 5 6 7 8 9 10**

COSO 1992 Control Element	Degree Evidenced for Reliable Financial Reporting
3.7 Controls Over Information Systems • Data Centre • Application Development & Maintenance • System Software • Access Security • Application Controls	**1 2 3 4 5 6 7 8 9 10**
4. INFORMATION AND COMMUNICATION	**Low High**
4.1 Information	**1 2 3 4 5 6 7 8 9 10**
4.2 Communication	**1 2 3 4 5 6 7 8 9 10**
5. MONITORING	**Low High**
5.1 Ongoing Monitoring	**1 2 3 4 5 6 7 8 9 10**
5.2 Separate Evaluations	**1 2 3 4 5 6 7 8 9 10**
5.3 Reporting Deficiencies	**1 2 3 4 5 6 7 8 9 10**
Note: Numeric references above are not part of COSO 1992. This is an interpretation of COSO 1992 and has not been evaluated or considered by the COSO Committee. Also, see COSO Small Business Control Criteria in Attachment 12.	

ATTACHMENT 12
SAMPLE COSO SPC
CONTROL CRITERIA CENTRIC ASSESSMENT EXAMPLE

COSO Smaller Public Company Principle	Degree Evidenced for Reliable Financial Reporting
CONTROL ENVIRONMENT	**Low** **High**
1. **Integrity and Ethical Values** – Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.	**1 2 3 4 5 6 7 8 9 10**
2. **Board of Directors** – The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.	**1 2 3 4 5 6 7 8 9 10**
3. **Management's Philosophy and Operating Style** – Management's philosophy and operating style support achieving effective internal control over financial reporting.	**1 2 3 4 5 6 7 8 9 10**
4. **Organizational Structure** – The company's organizational structure supports effective internal control over financial reporting.	**1 2 3 4 5 6 7 8 9 10**
5. **Financial Reporting Competencies** – The company retains individuals competent in financial reporting and related oversight roles.	**1 2 3 4 5 6 7 8 9 10**
6. **Authority and Responsibility** – Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control over financial reporting.	**1 2 3 4 5 6 7 8 9 10**
7. **Human Resources** – Human resource policies and practices are designed and implemented to facilitate effective internal control over financial reporting.	**1 2 3 4 5 6 7 8 9 10**

COSO Smaller Public Company Principle	Degree Evidenced for Reliable Financial Reporting
RISK ASSESSMENT	**Low** **High**
8. **Financial Reporting Objectives** – Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting.	**1 2 3 4 5 6 7 8 9 10**
9. **Financial Reporting Risks** – The company identifies and analyzes risks to the achievement of financial reporting objectives as a basis for determining how the risks should be managed.	**1 2 3 4 5 6 7 8 9 10**
10. **Fraud Risk** – The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.	**1 2 3 4 5 6 7 8 9 10**
CONTROL ACTIVITIES	**Low** **High**
11. **Integration with Risk Assessment –** Actions are taken to address risks to the achievement of financial reporting objectives.	**1 2 3 4 5 6 7 8 9 10**
12. **Selection and Development of Control Activities** – Control activities are selected and developed considering their cost and potential effectiveness in mitigating risks to the achievement of financial reporting objectives.	**1 2 3 4 5 6 7 8 9 10**
13. **Policies and Procedures** – Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in management directives being carried out.	**1 2 3 4 5 6 7 8 9 10**
14. **Information Technology** – Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.	**1 2 3 4 5 6 7 8 9 10**
INFORMATION AND COMMUNICATION	**Low** **High**
15. **Financial Reporting Information** – Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that supports the achievement of financial reporting objectives.	**1 2 3 4 5 6 7 8 9 10**

COSO Smaller Public Company Principle	Degree Evidenced for Reliable Financial Reporting
16. **Internal Control Information** – Information needed to facilitate the functioning of other control components is identified, captured, used, and distributed in a form and timeframe that enables personnel to carry out their internal control responsibilities.	**1 2 3 4 5 6 7 8 9 10**
17. **Internal Communication** – Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.	**1 2 3 4 5 6 7 8 9 10**
18. **External Communication** – Matters affecting the achievement of financial reporting objectives are communicated with outside parties.	**1 2 3 4 5 6 7 8 9 10**
MONITORING	**Low High**
19. **Ongoing and Separate Evaluations** – Ongoing and/or separate evaluations enable management to determine whether the other components of internal control over financial reporting continue to function over time.	**1 2 3 4 5 6 7 8 9 10**
20. **Reporting Deficiencies** – Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.	**1 2 3 4 5 6 7 8 9 10**

ATTACHMENT 13
SAMPLE MANAGEMENT
REPRESENTATION ON ICOFR

We, the undersigned, acknowledge that we have:

(1) Responsibility for developing and maintaining internal controls and disclosure controls that provide reasonable assurance that ABC's financial statements and supplemental SEC disclosures present fairly the results of operation and the financial position of ABC Inc. in accordance with generally accepted accounting principles and other applicable SEC regulation.

(2) Responsibility for overseeing that the organization has cost effective risk and control management systems that provide reasonable assurance ABC's external financial disclosure objectives will be achieved.

(3) Reviewed the significant control and risk issues identified by work units and management through the company's risk and control self-assessment process, and the significant issues identified by our Internal Audit department and our External Auditor, Smith & Jones, that have been brought to our attention. We have initiated steps to adjust controls in areas where the error rates and/or residual risks identified related to the non-achievement of ABC's disclosure objectives were considered to be excessive and/or unacceptable.

(4) Reviewed our process to manage risk and control and this year's report on our risk management process prepared by our Internal Audit for the Audit Committee. We are satisfied that our risk and control assessment framework process provides our Audit Committee and our External Auditors, Smith & Jones, with a reliable and materially complete report on the status of risk and controls related to our external disclosure objectives as required by Sections 302 and 404 of the Sarbanes-Oxley Act of 2002.

_____ _____

CEO CFO

ATTACHMENT 14
SAMPLE CONTROL DEFICIENCY GRADING SYSTEM

EC – Excessive Controls

0 Fully Acceptable - No unacceptable concerns. No additional attention or corrective actions required at the current time.

1 Low - Inaction on unacceptable terms could result in minor negative impacts. Routine attention required to adjust status to an acceptable level.

2 Moderate - Inaction on unacceptable items could result in or will allow continuation of mid-level negative impacts. Moderate effort required to adjust status to an acceptable level.

3 Significant - Inaction on unacceptable items could result in or will allow continuation of serious negative impacts. Attention required immediately to adjust status to an acceptable level.

4 Major - Inaction on unacceptable items virtually certain to result in or allow continuation of very major negative consequences. Analysis and corrective action required immediately (SOX Significant Deficiency rating for ICoFR).

5 Severe - Inaction on unacceptable items virtually certain to result in or allow continuation of very severe negative impacts. Senior level attention urgently required (SOX Material Weakness rating for ICoFR).

6 Catastrophic - Inaction on unacceptable items will result in or allow the continuation of catastrophic proportion impacts. Senior level attention urgently required to avert a catastrophic negative impact on the organization.

7 Terminal - The current status is already extremely material and negative and having disastrous impact on the organization. Immediate top priority action from all key players will be necessary to prevent the total elimination of the entity.