

Sarbanes-Oxley Sections 302 & 404

A White Paper Proposing Practical, Cost Effective Compliance Strategies

Prepared by:

Tim J. Leech, FCA-CIA, CCSA, CFE



2655 North Sheridan Way, Suite 150
Mississauga, Ontario, Canada, L5K 2P8
Tel: 905 823-5518 Fax: 905 823-5657
Tim.Leech@carddecisions.com
www.carddecisions.com

April 2003

Complying with Sarbanes-Oxley Sections 302 & 404

Table of Contents

EXECUTIVE SUMMARY	1
ABOUT THE AUTHOR	2
PREFACE.....	3
INTRODUCTION	4
VISUALIZING THE GOALS OF SECTIONS 302 and 404.....	6
LINKING SECTION 302 TO THE 302/404 OVERVIEW	8
LINKING SECTION 404 TO THE 302/404 OVERVIEW	11
WHAT'S WRONG WITH THE STATUS QUO?	13
PRACTICAL AND COST EFFECTIVE 302/404 COMPLIANCE STRATEGIES	15
CAUTIONS TO CONSIDER	21
WHAT THE FUTURE HOLDS	23

List of Attachments

SOX Sections 302 & 404: Full Text	1
SOX Assurance Strategies - Options Overview	2
Basel Bank Governance Deficiencies Summary	3
Control Models	4
Risk Source Models	5
Risk & Control Assessment Approach Overview	6
Risk Management Capability Assessment Criteria	7
SOX 302/404 Quality Assurance Strategies	8
Sample Management Representation to Audit Committee	9
What's Wrong with the Status Quo? - Detailed Comments	10
Contrasting Traditional Assurance Strategies and ERAM	11

EXECUTIVE SUMMARY

The Sarbanes-Oxley Act of 2002 ("SOX") imposes significant new requirements on companies listed on U.S. stock exchanges. These rules are particularly radical in the areas of assessment and oversight of control systems that support external financial disclosures.

Regulatory requirements related to internal control representations have been around in various forms, in various business sectors, for many years. The new component causing significant consternation in the business community is that a company's external auditor, for the first time, must provide an annual opinion on the reliability of the control representation made by a company's CEO and CFO. Simply put, there must now, perhaps for the first time in a serious way, be a sound, demonstrable and persuasive basis for the CEO/CFO representations on control status.

Since SOX was passed in July of 2002, tens of thousands of pages have been written on the implications of this legislation, interpretations of the legislation, and the specific implementation plans of the various enforcement agencies, including the SEC, charged with applying these new laws. Although there are a number of contentious SOX sections that have created debate, comments and objections, sections 302 and 404 create the most radical, ongoing and potentially onerous compliance obligations. Other countries may follow the U.S.' lead and impose requirements similar to those in sections 302 and 404.

This paper sets out a point-by-point interpretation of the requirements imposed by these sections and provides practical, cost effective recommendations to respond. Traditional audit/compliance approaches and tools in use in most companies today are woefully inadequate to meet the virtually "real time" assessment and monitoring expectations imposed by sections 302 and 404. The strategies proposed in this paper, to be cost effective and add value, require the adoption of enterprise risk and control assessment and monitoring technology. Real value will only be realized when the assessment and monitoring systems linked to SOX are also used to foster continuous improvement, keep control costs as low as possible, and maintain residual risks at acceptable levels.

Three strategies are proposed to prepare for the audit of the CEO/CFO control representation required by section 404. These include a "big picture" macro level risk and control assessment related to a company's entire external disclosure process; a more rigorous documentation, prioritization and assessment of the sub-processes that support SEC 10K and 10Q disclosures; and, for those looking for a "quick fix", a minimalist approach to compliance, albeit with some significant legal and cost/benefit caveats that need to be carefully considered. Although the first two strategies will require significant culture and role change, they can still be accomplished fairly quickly and at a modest cost. The third option can appear, at least initially, to be a cheaper option, but may have significant hidden costs and provide limited payback.

The paper closes with four cautions companies and their advisors should carefully consider when developing a SOX 302/404 compliance framework and some "best guesses" of what the future holds in this area.

ABOUT THE AUTHOR

Tim J. Leech, FCA-CIA, CCSA, CFE, MBA

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

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

Some of Leech's experiences and achievements include:

- pioneering and developing a work team driven approach to control and risk management and reporting that has been recognized globally as a leading edge, control and risk management tool;
- developing Collaborative Assurance and Risk Design[™] training methods and software used by major organizations around the world. Some of the organizations that have acquired licences over the past decade to use CARD[®] training tools internally include: Royal Bank, BellSouth, British Gas, Shell U.K., Georgia-Pacific, NatWest Bank, University of California, CIBC, Mobil, Cabot Corporation,, Ansett Airlines, TD Bank, NorthEast Utilities, Chiquita Brands, Compart, City of Detroit, Telephone and Data Systems, Telstra, Western Mining, Royal Bank, Canada Life, and Australian Taxation Office;
- numerous T.V. appearances, a national radio show, and a monthly column on control, ethics, and fraud related topics;
- authoring technical papers in response to exposure drafts of control governance studies in the U.S., the U.K., and Canada including reports by the Treadway Commission, COSO, Cadbury, and CoCo internal control research projects, the Sarbanes-Oxley legislation passed in the U.S. in 2002, and the new professional standards issued by IIA;
- developing technical material for research studies on CSA/CRSA including the IIA report CSA: Making the Choice, and the IIA research study CSA: Experience, Current Thinking and Best Practices and a text published by John Wiley titled "Control Self-Assessment for Risk Management and Other Practical Applications";
- delivery of expert witness services and testimony during civil and criminal actions related to fraud, secret commissions, conflict of interest, breach of contract, and officer/director due diligence;
- developing training tools that have proven effective in a wide range of nationalities and cultures. Training on CARD[®] methods and tools is available in English, Spanish, Greek, and French through Oxley Fitzpatrick in the U.K., Rosés Auditores in Spain, Harborview Partners in the U.S., and participating KPMG and E&Y offices located around the world;
- member of the IIA Enterprise Risk Management & Self-Assessment Advisory Panel and author of the IIA CCSA practice exam; and
- primary author and developer of CARD[®] *map* software - the world's first Collaborative Assurance and Risk Design[™] groupware. CARD[®] *map* software is used by major companies and public sector organizations around the world.

PREFACE

I started my career as an apprentice external auditor with Coopers & Lybrand (now Pricewaterhouse Coopers) in 1979. Since that time I have worked as an internal auditor, corporate accounting manager, forensic accountant, Director of a control and risk management consulting practice, Managing Director of an international control and security firm and, for the last 12 years, CEO of a firm specializing in enterprise risk and assurance training, consulting, and software. Over those many years, there has never been an instance in memory where a corporate governance reform has produced a response of the magnitude and gravity provoked by the Sarbanes-Oxley Act of 2002. This legislation impacts in a significant way on regulators, boards of directors, senior management, personnel all across an organization, lawyers, investment dealers, external and internal auditors, credit agencies, foreign governments, and many others. The Sarbanes-Oxley Act ("SOX") represents the highest corporate governance compliance bar raised anywhere in the world to date.

The legislation has produced a veritable blizzard of interpretations and editorials from journalists, law firms, public accounting firms, internal auditors, academics and others. As I prepared to write this paper, my research covered the legislation, interpretations of the legislation from the Securities Exchange Commission ("SEC"), interpretations and commentary on the SEC interpretations from CFOs, major legal and accounting firms and others, editorials written by business journalists, and more. As I waded through this rapidly expanding body of literature and "expert advice", and fielded questions from public companies all across North America, it became increasingly clear that many companies are confused and looking for an understandable and practical interpretation of the legislation, particularly with respect to compliance with sections 302 and 404. This paper explains, in as simple terms as is possible, SOX sections 302 and 404 of SOX and provides practical, cost effective suggestions for companies that want to comply with these new rules.

I hope you find my paper interesting and useful. If you have criticisms, suggestions or comments on this paper and are prepared to share them, please e-mail them to me at Tim.Leech@carddecisions.com. Feedback on this White Paper, both positive and negative, will be posted in the Industry Info/Articles section of our web site www.carddecisions.com.

I would also like to extend special thanks to my technical review panel including my partner, Bruce McCuaig, Mike Corcoran, CEO Harborview Partners, Parveen Gupta, Associate Professor Lehigh University, Larry Hubbard, CEO Larry Hubbard & Associates, and Jon Elks, SVP Risk Management and Assurance Cablevision. Their assistance on this paper is greatly appreciated. Any deficiencies in the paper are entirely my own.

Tim Leech FCA·CIA, CFE, CCSA
April 2003

INTRODUCTION

In October of 1987 the Report of the Commission on Fraudulent Financial Reporting, better known as the Treadway Commission report, made the following recommendation:

For the top management of a public company to discharge its obligations to oversee the financial reporting process, it must identify, understand, and assess the factors that may cause the financial statements to be fraudulently misstated.

The stated mission of the Treadway Commission was “to identify causal factors that can lead to fraudulent financial reporting and steps to reduce its incidence.”

As a result of the Treadway Commission, the SEC proposed rules in 1988 that bear striking similarities to SOX sections 302 and 404. As a direct result of an aggressive counter lobby from a wide range of interest groups these proposals were not enacted.

Following the recommendations of the Treadway Commission, the five professional groups in the U.S. that sponsored Treadway developed a control framework titled "Committee of Sponsoring Organizations Internal Control - Integrated Framework" (commonly known as "COSO"). COSO was intended to help public companies, their auditors, advisors, and regulators better understand the key elements of an effective control framework. COSO was released in final in September of 1992.

The dawn of the 21st century brought with it a spate of new disasters that make the governance problems that led to the creation of the Treadway Commission seem trivial in comparison. Massive corporate governance failures at Enron, WorldCom, Adelphia, Allied Irish Bank, HealthSouth and many other large firms shook the confidence of shareholders, lenders, regulators, and the public with respect to the integrity of senior management, competency of boards of directors, integrity of external auditors, lawyers, investment dealers, and others and, more generally seriously impacted on the confidence of investors in the reliability of external disclosures of listed public companies.

In light of this massive reoccurrence of fraudulent and unreliable financial reporting, U.S. Congress concluded that the few tangible corrective actions that had been taken voluntarily by the private sector since the issuance of the Treadway recommendations in 1987 were not enough. In particular, Congress wanted to redefine a new and more independent auditor/company relationship with significantly more emphasis on the role of the board of directors to oversee and safeguard the reliability of external disclosures and independence of external auditors charged with reporting on those corporate disclosures.

The result of this growing realization was passage of the Sarbanes-Oxley Act of 2002 in July 2002.

Two of the sections of SOX that pose particularly significant implementation and compliance challenges are sections 302 and 404. Attachment 1 to this paper contains the full text of these two sections.

Simply put, these sections require that the CEO and CFO of an organization certify and assert to stakeholders that SEC disclosures, including the financial statements of the company and all supplemental disclosures, are truthful and reliable, and that management has taken appropriate steps to satisfy themselves that the disclosure processes and controls in the company they oversee are capable of consistently producing financial information stakeholders can rely on (Section 302). The company's external auditor must report on the reliability of management's assessment of internal control (Section 404).

SEC Commissioner Cynthia Glassman summarized the intent of these sections in a speech on September 27, 2002 to the American Society of Corporate Secretaries.

Recognizing that awareness must precede action, Sarbanes-Oxley and the Commission's rules require the CEO and Board to make certain that procedures are in place to ensure that they hear bad news. Under the Commission's recently adopted rules, these procedures must ensure that all material information - both financial and non-financial – gets to those responsible for reporting it to the investing public.

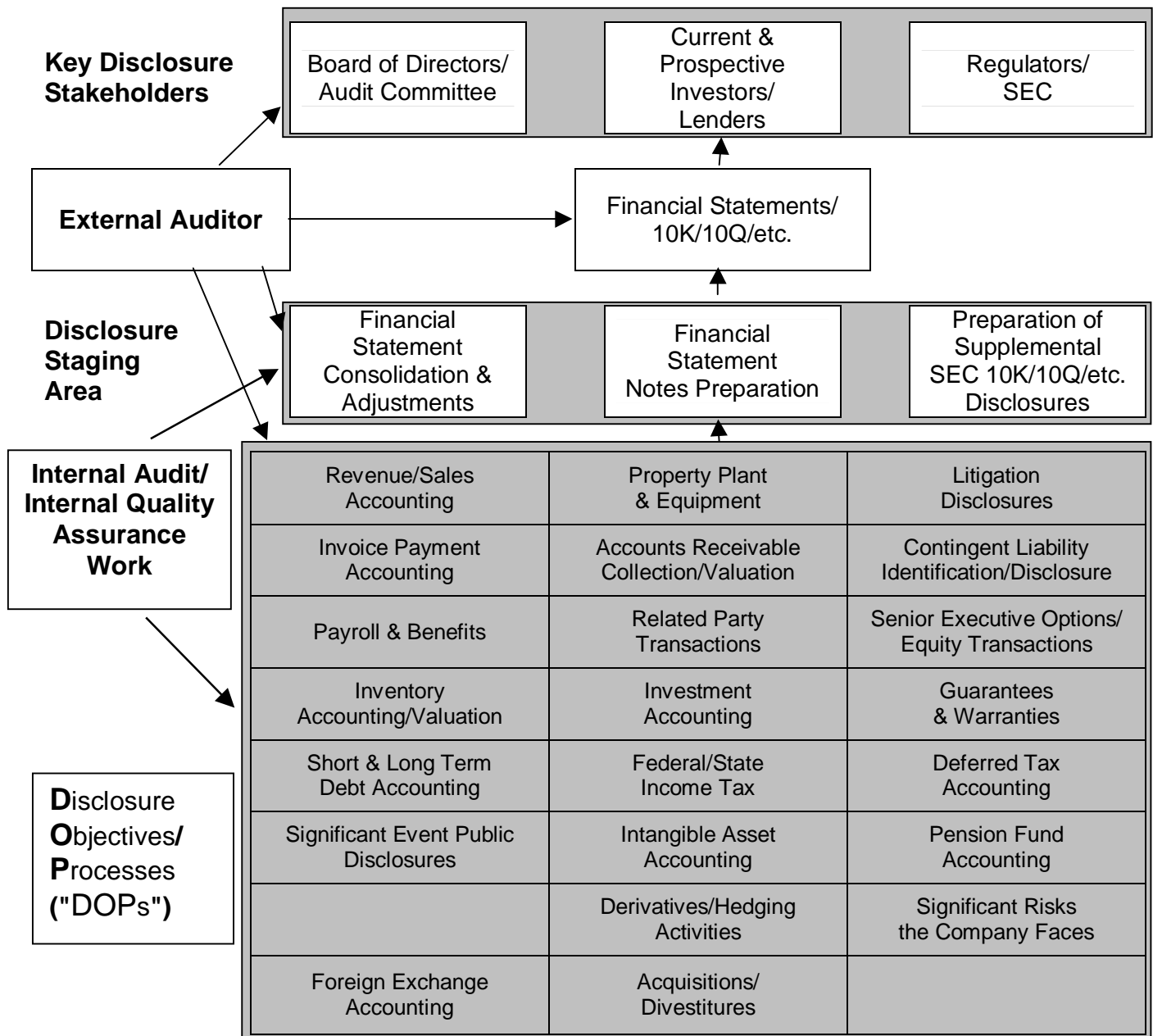
This paper demystifies and interprets SOX sections 302 and 404 and provides practical, cost effective suggestions and cautions companies can use to respond to these radical new governance requirements. It is not a legalistic interpretation of the legislation, but rather a common sense rendition of a fairly complex and radical piece of legislation.

VISUALIZING THE GOALS OF SECTIONS 302 and 404

The fundamentals of sections 302 and 404 can be explained using the diagram below. The primary goal of the disclosure system is summarized in the purpose statement of SOX:

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

Sarbanes-Oxley Section 302 & 404 Overview



For key stakeholders to evaluate any organization, be it a bank, insurance company, oil company, manufacturer, retailer, health care provider, etc., 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. The primary goal of the legislation can be stated positively:

Ensure that SEC filings including financial statements, notes, and supplemental disclosures, are reliable.

Primary data sets used by the various disclosure stakeholders are monthly, quarterly, and annual financial statements, notes to the financial statements, and the many supplemental disclosures required by the SEC in 10K and 10Q filings. 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 302/404 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 SEC 10K/10Q/and Other 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. A few are done manually and involve significant levels of judgment. The DOPs must deliver generally reliable and complete information to the Disclosure Staging Area for the final consolidated package to be reliable. Some of the DOPs are particularly significant and capable of creating material and dangerous disclosure problems. Others are less critical.

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 recent examples include Enron, WorldCom, Xerox, and HealthSouth. Particular attention needs to be paid to ensuring there are adequate controls in place to ensure that senior level executives, including CEOs and CFOs, do not improperly force staff to make inappropriate adjustments in the Disclosure Staging Area prior to release to Key Disclosure Stakeholders.

LINKING SECTION 302 TO THE 302/404 OVERVIEW

To focus senior executives on their responsibility for reliable external disclosures Congress enacted SOX section 302. A point-by-point analysis of this section follows.

Section 302 Requirement	Link to the Overview
302(a)(1) the signing officer has reviewed the report	CEO and CFO must review SEC disclosures shipped from the Disclosure Staging Area to Key Disclosure Stakeholders.
302(a) (2) based on the officer’s knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;	The CEO and CFO must not allow any SEC disclosures to be shipped to stakeholders from the Disclosure Staging Area with falsehoods or omissions. The "omit to state" portion of this section means that the CEO and CFO must take steps to ensure that the flow from the DOPs is reliable and complete.
302(a)(3)based on such officer’s knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;	This requirement suggests that the disclosures to key stakeholders must be more than just being in compliance with generally accepted U.S. accounting principles - they must “ fairly present in all material respects ”. This could mean that, in a case like Enron, if the use of Special Purpose Entities caused the statements to not “fairly present in all material respects”, but they were still technically in accordance with U.S. generally accepted accounting principles, this would need to be corrected.
302(a)(4)(A) the signing officers—are responsible for establishing and maintaining internal controls	The CEO and CFO are responsible for setting up and maintaining appropriate and sufficient controls in the Disclosure Staging Area and for the universe of DOPs to ensure timely and reliable external disclosures.
302(a)(4)(B) the signing officers —have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;	The CEO and CFO must be confident that there are adequate controls to ensure that timely and reliable information is flowing to the Disclosure Staging Area related to all key DOPs. For example, if a material lawsuit was launched against the company in a foreign subsidiary, the system must be capable of identifying the situation on a timely basis and feeding the necessary information to the Disclosure Staging Area.

Section 302 Requirement	Link to the Overview
<p>302(a)(4)(C) the signing officers — have evaluated the effectiveness of the issuer’s internal controls as of a date within 90 days prior to the report; and</p>	<p>This is one of the most serious and onerous requirements imposed by SOX. The CEO and CFO are expected to be able to demonstrate that there is a reliable process in place to evaluate, at least quarterly, the controls in place to ensure the reliability of the data being produced by the Disclosure Staging Area and all DOPs. It is important to note that looking at controls in a vacuum without understanding and evaluating the risks that threaten disclosure objectives will produce sub-optimal results and is inconsistent with the principles in the new draft COSO framework scheduled for release in April 2003. The omission of risk identification and assessment in the assessment process should be considered a significant risk in its own right. Very few companies have formally documented the end result DOPs that support SEC disclosures, the risks to those DOPs, the controls used to mitigate those risks, and current performance data (i.e. the frequency that the Disclosure Staging Area(s) and DOPs produce errors or omissions).</p>
<p>302(a)(5)(A) the signing officers have disclosed to the issuer’s auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)----all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer’s ability to record, process, summarize, and report financial data and have identified for the issuer’s auditors any material weaknesses in internal controls; and</p>	<p>The CEO and CFO must be aware of and report to their external auditor and Audit Committee the Disclosure Staging Area(s) and/or DOPs that are producing, or may produce as a result of serious control deficiencies, unreliable and/or incomplete information. It is important to note that the vast majority of companies, at any point in time, have Disclosure Staging Areas and/or some number of DOPs that produce inaccurate or incomplete information. Companies that say they have no control problems should be considered high potential candidates for a corporate governance disaster. Healthy companies recognize, acknowledge, and address the fact there are always control problems - problems that can, but only rarely do, preclude reliable external disclosures.</p>

Section 302 Requirement	Link to the Overview
<p>302(a)(5)(B) the signing officers have disclosed to the issuer’s auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function) -----any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer’s internal controls; and</p>	<p>This section requires that the CEO and CFO advise the external auditor and audit committee of any situation, regardless of materiality, that indicates dishonesty on the part of any employee that works in a Disclosure Staging Area or plays a significant role in any of the controls that support any of the DOPs that feed the Disclosures Staging Area(s). An example would be if the Controller of a subsidiary is caught falsifying an expense report, putting in an accrual for a liability that had not yet been incurred, or recognizing a sale in the accounts that had not yet been earned. Strictly interpreted, all of these situations would be a reportable item under this section. Depending on how broadly the SEC interprets "employees who have a significant role in the issuer's internal controls", this rule may apply to hundreds of employees that play a significant role in Disclosure Staging Areas, business operations, or any of the DOP control systems.</p>
<p>302(a)(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.</p>	<p>This section requires that in any situation where controls were evaluated at a point in time and subsequently an event occurs that could impact in a significant way on the controls or the reliability of the control processes, this must be documented and reported by the CEO and CFO, including any steps underway to correct it. Presumably, the company must have a system in place capable of scanning the disclosure/risks/ controls universe and detecting significant changes. It isn’t clear from the wording whether this is a “to the best of my knowledge” law, with no requirement to positively seek information as to whether changes in the risk/control universe have occurred, or a more onerous expectation that positive steps must be taken by the company to identify significant changes in the control environment.</p>

LINKING SECTION 404 TO THE 302/404 OVERVIEW

Section 404 adds further emphasis to Section 302 by requiring an annual management assessment of controls and an external audit or opinion on its reliability.

Section 404 Requirement	Link to the Overview
<p>S404(a)(1)(2) RULES REQUIRED.</p> <p>The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 to contain an internal control report, which shall—</p> <ul style="list-style-type: none"> (1) state responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) contain 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. 	<p>This section requires that there be a report that</p> <ul style="list-style-type: none"> (1) formally acknowledges the responsibility of management for creating and maintaining controls to manage the risks that could cause inaccurate, incomplete or fraudulent data to be shipped from the Disclosure Staging Area(s) or from any of the significant DOPs, and (2) contains an assessment of the reliability of the controls in the Disclosure Staging Area(s) and DOPs to manage risks that could cause, or result in, inaccurate, incomplete and/or fraudulent disclosures being released to key stakeholders. <p>The SEC proposed the content and format of these assertions in the fall of 2002 and will soon be finalizing the specific wording that must be used.</p>
<p>S404(b) INTERNAL CONTROL EVALUATION AND REPORTING.</p> <p>With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An</p>	<p>The external auditor must provide an opinion on the reliability of the assessment developed by management in section 404(a)(2). This requires an audit opinion on the reliability of the management representations on the effectiveness of the controls in the Disclosure Staging Area(s), and controls used to ensure that the DOPs, collectively, generate reliable disclosures for key stakeholders. Although there is a strong bias in the wording, and in many interpretations of the wording, that management will assert that controls are “adequate” or “effective”, presumably it would also be acceptable, and much more plausible, if management disclosed in their</p>

Section 404 Requirement	Link to the Overview
<p>attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.</p>	<p>assessment Disclosure Staging Areas and DOPs that have significant levels of process variability or error rates. The external auditor would then agree or disagree with that assessment much the same way an auditor can give a clean opinion on financial statements that disclose a very bad year in terms of financial results. Once information on process variability/error rate in Disclosure Staging Areas or DOPs is disclosed to the external auditor, the onus would then be on the external auditor to decide if they are still able to give a clean opinion on the financial statements, whether additional work is required by management and/or the external auditor to compensate for the process quality problem from the DOPs and/or Disclosure Staging Areas, or if they are precluded from issuing a "clean report" on the accounts.</p>

WHAT'S WRONG WITH THE STATUS QUO?

In most situations, when a government enacts new legislation and regulation of the significance and impact of SOX, it indicates the government of the day believes the existing corporate governance regulatory framework has failed, and failed badly. This conclusion has been reached to varying degrees by regulators in the U.S., U.K., Australia, Canada, Europe, South Africa and elsewhere.

The Basel Committee, part of the Bank for International Settlements, has been working since 1998 on the development of a new corporate governance framework to address what they consider to be an ineffective and broken corporate governance regime. (Note: this work is generally known as Basel Capital Accord II). Basel identified a list of key governance deficiencies present in banks in countries all over the world that have been involved in significant frauds and/or control breakdowns. Many of the corporate governance problems identified by Basel in banks globally have also been present in recent corporate sector disasters including Enron, WorldCom, Allied Irish Bank, HealthSouth, and others. The Basel listing of bank corporate governance deficiencies and a summary of the "Sound Practices" Basel has proposed to address them is included as Attachment 3 to this paper.

In addition to the problems identified by the Basel governance study, a summary of personal observations on what's wrong with the status quo drawn from over 20 years working with companies around the world is included as Attachment 10. The SOX 302/404 recommendations proposed in this paper are an attempt to address as many of these deficiencies as possible, while still creating a cost effective compliance program that adds value.

The deficiencies identified by the Basel Committee in Attachment 3 and the issues identified in Attachment 10 must all be addressed over the longer term to restore and maintain the confidence of the investment community.

EVALUATING THE BUSINESS CASE FOR SOX COMPLIANCE

Today's business environment is challenging to say the least. There is continuous pressure and demands from customers, competitors, regulators, unions and other key stakeholders. Time and money are scarce commodities that need to be used wisely.

While acknowledging that the administrative burden imposed by SOX is a consideration, the SEC has indicated that they will not tolerate companies that do not make sincere and genuine efforts to evaluate the risk and control management systems that support the reliability of external disclosures. There will be even less tolerance for companies that allow the issuance of inaccurate and/or fraudulent disclosures and are later caught. SEC Commissioner, Cynthia Glassman, in a speech to the American Society of Corporate Secretaries stated:

“one factor we will look at is whether the company took seriously its obligation to detect fraud. Obviously, no system of controls can prevent all misconduct; however, if a company can demonstrate that it has satisfied its obligation to implement good procedures, then in my eyes it has a significant better chance of receiving leniency (assuming the other criteria set out in the report are met) In short, if you are looking for leniency you had better be able to show that you cared about preventing corporate misconduct before you discover that it occurred.”

Putting aside for a moment “We have to comply with Sarbanes-Oxley, it’s the law” and/or “If we don’t comply and are caught our officers and directors could face fines and jail time”, SOX presents an opportunity that can help transition an organization from traditional, silo based risk and control approaches to integrated, Enterprise-wide Risk and Assurance Management (‘ERAM”). An overview of the differences between a traditional, silo-based approach to risk and control management and ERAM is included in Attachment 11 to this paper. Significantly more value can be derived from existing assurance functions/activities by adopting new and better assurances methods and tools to identify root causes of current and potential control breakdowns. The business case for going beyond the “letter of the law” and adopting the spirit of SOX and a broader ERAM approach is steadily gathering support around the world.

PRACTICAL AND COST EFFECTIVE 302/404 COMPLIANCE STRATEGIES

Practical, cost effective recommendations to comply with SOX sections 302 and 404 follow.

RECOMMENDATION #1- Evaluate at a macro level the risks, controls, and residual risk status over the entire SEC 10K/10Q external disclosure process.

Since many of the biggest disasters in corporate governance history have occurred in the Disclosure Staging Area, it makes sense to focus on “the big picture” and the “really big risks” first. A macro level analysis of section 302/404 disclosure risks and controls can usually be accomplished quite quickly through self-assessment forums or, if self-assessment is not a good fit for the current corporate culture, more traditionally in a collaborative way using in-house assurance specialists or an external consultant. An experienced risk and assurance consultant should be able to complete a macro level SOX analysis using traditional data gathering and audit techniques in less than 20-30 days of work even in a fairly large company.

The approach involves creating a formal, documented assessment of the risks, controls and residual risk status related to the macro level objective to:

Ensure SEC 10K and 10Q disclosures are complete and reliable.

The core elements of a risk and control assessment are shown in Attachment 6.

The analysis starts by documenting a list of key risks to this macro level objective. These are then ranked in terms of likelihood, consequence, mitigation estimate/control effectiveness, and residual risk status. Steps should be taken to ensure that fundamental risks that have caused major failures elsewhere are included in the evaluation. (e.g. “Executive compensation system increase pressure on senior executives to manage/distort profit”, “External auditors are not current on SEC disclosure rules”, “External auditors lose objectivity due to commercial pressures and partner reward systems”, “Material breach of debt covenant not identified”, “Key employees lie about critical disclosure information”, etc). The use of a Risk Source model and a range of completeness techniques to identify the key risks that threaten this micro objective are strongly recommended.

An overview of three sample Risk Source Models is included in Attachment 5. The use of risk identification completeness aids should be considered mandatory. If an important risk is missed, the reviewer/auditor will not look for and evaluate the controls in place/use to manage it. The new COSO Enterprise Risk Management Conceptual Framework scheduled for release in draft in the spring of 2003 attaches great importance to the role of risk analysis in a company's macro control framework. The

new version of COSO should provide an excellent source of guidance for companies developing SOX compliance programs.

The next step is to identify the controls currently in use/place to mitigate the risks identified. The use of a control model is strongly recommended for this step. Most comment letters filed in response to the draft SEC implementation guidance for SOX section 404 (RIN 3235-A166) from large public accounting firms and the AICPA strongly advocate the use of “control criteria”, a documented and acknowledged control framework, when making and reporting on control representations.

Sample control models are included as Attachment 4. COSO, the Canadian CoCo and the international CARD[®] *model* frameworks and others can all be used to help evaluate internal controls. The original 1992 COSO framework works very well when evaluating the macro level control framework for the enterprise as a whole, but can be more difficult to apply on an individual objective or when searching for a control to mitigate a specific risk. For macro level control evaluations readers should consult the September 1992 Evaluation Tools volume of COSO, page 201. COSO capabilities in this area will be significantly enhanced with the release of the updated COSO framework scheduled for release in draft in the draft of 2003. The “NEW AND IMPROVED COSO” is expected to include the following components: analysis of the internal environment, event identification, risk assessment, risk response, control activities, information and communication, monitoring, limitations and roles, and responsibility sections. (Source: COSO presentation, IIA GAM Conference, March 2003)

After risks and controls have been identified, documented and evaluated, the next step is to document a picture of the current risk situation after existing controls are considered, including information on current “Process Reliability/Variability”. This step includes identifying Key Process Indicators (“KPIs”) or Process Reliability/Variability data. This information includes such things as the number and dollar value of adjustments to the accounts that have been made following external audit testing, (i.e. adjustments to the accounts or supplemental disclosures identified by the external auditor or caught through internal processes prior to approving the disclosure package), the number and dollar value of adjustments that are made in key accounting/disclosure processes that relate to prior periods, (i.e. mistakes/omissions found in prior periods), and any other information that helps answer the question of “What do we know right now about the reliability and completeness of the processes that provide data to assemble financial statements, the notes to the financial, and the supplemental SEC disclosures.” This approach is entirely consistent with analysis techniques advocated by leading quality systems like Baldrige, Six Sigma and ISO 9000.

In cases where unacceptable residual risk concerns are identified, action plans must be developed to address them.

The use of an automated computer system to capture this macro level analysis, track progress addressing any unacceptable risks, and monitor risk and control status in future periods is strongly recommended to meet quarterly status analysis requirements

and keep costs to a minimum. There are a variety of software packages on the market designed for this purpose and more are emerging. Offerings in this space include CARD[®] *map* software offered by CARD[®] *decisions*, Risk Navigator offered by Paisley, fORM from Methodware, Horizon from JPMorganChase, Visual Assurance from Kilcare, Magique from Horwath Software, Risk Prism offered by PwC, and others.

It is essential when completing this macro level analysis to document and evaluate the "big picture" controls. "Big picture" controls are designed to manage the most significant risks and prevent inappropriate senior executive override, including the role played by any internal disclosure committee or process, the role of the audit committee, the role of the external auditor, the role of in-house and external legal counsel related to significant disclosures, the rigor and reliability of the process used by the CEO and CFO to support their sign-off of disclosures, the reward/punishment system to encourage truthful disclosures and discourage fraudulent and/or excessively aggressive disclosures, high level reasonability assessments done by analysts, performance monitoring activities, and other significant controls. Although controls such as general ledger account analysis and reconciliation, consolidation checklists and sign-offs, passwords, and other traditional controls are easily audited, they are not the major controls capable of preventing disasters like Enron, WorldCom, HealthSouth and others.

RECOMMENDATION #2 – UTILIZE TECHNOLOGY TO PROVIDE SUPPORT FOR SOX 302/404 REPRESENTATIONS

The use of technology to support SOX compliance programs helps integrate the efforts of all assurance providers, facilitates preparation, analysis and quarterly monitoring of the consolidated risk and control position, encourages the participation of work unit personnel, and provides an easy to use platform for assurance work performed by internal and external auditors. Key steps to implement an automated SOX 302/404 compliance system follow.

1. In addition to completing the macro, "big picture" risk and control analysis outlined in Recommendation #1, document the universe of significant DOPs (Disclosure Objectives/Processes) that feed the Disclosure Staging Area. See page 5 of this paper for an illustrative overview of DOPs. This overview can also be depicted as a collection of business processes that feed the Disclosure Staging area. It is better for purposes of risk and control assessment if the DOPs are stated as end result objectives to stress the outcomes required. Whenever possible, identify a DOP owner or sponsor in business units and/or Disclosure Staging Area that has lead responsibility for assessing the risk and control status for each DOP. Accountability, combined with an effective monitoring/oversight program, are key elements of a solid compliance framework.
2. Decide whether primary documentation/assessment work necessary to support external control representations will be completed and maintained by work unit personnel or risk and control assurance specialists, such as internal audit and/or

contract assurance personnel. (NOTE: It can be quite expensive to maintain current, quarterly updated data using assurance specialists/auditors alone) An overview of 10 different assurance approaches that can be used is included as Attachment 2. To meet the requirement for timely and continuous monitoring of risks and controls the use one or more self-assessment approaches combined with one or more direct report audit methods is strongly recommended. During the transition/implementation phase, Internal Audit and/or contract personnel can be used to help with the initial set-up of the necessary SOX risk and control documentation. After the initial documentation is complete, seriously consider assigning ongoing maintenance of the risk and control documentation of the DOPs to work unit personnel.

3. Rank the DOPs in terms of their “Importance” to consolidated external disclosures. Importance ratings are generally based on criteria such as materiality of the information produced by the DOP, consequences of a misstatement, and importance to stakeholders. Pay particular attention to DOPs and Disclosure Staging Area activities that involve high levels of judgment and/or where Generally Accepted Accounting Principles allow a range of treatment options. These are sometimes referred to as “Profit Adjustment Accounts”. Profit Adjustment Accounts are used, both legitimately and otherwise, for discretionary quarterly and annual profit smoothing or profit position optimization. These accounts are usually well known to both the corporate accounting personnel and experienced external auditors. There is growing pressure on audit committees to understand and monitor these "swing" accounts.
4. Gather and consolidate all of the information that is currently known about risks and controls related to the DOPs and input the information to the risk and assurance database. Risk and control information sources include corporate policy statements, work unit documentation, risk and control self-assessment documentation, internal audit reviews, any external specialist reviews done on complex topics such as derivatives, foreign exchange, complex tax issues, external audit control assessment documentation, and other data. Pay particular attention to gathering and documenting “best available” performance indicator data that provides insight in to the current reliability/variability of the DOPs and Disclosure Staging Areas. This approach to identifying and analyzing Key Performance Indicators on important DOPs is consistent with some of the new and better external audit methodologies in use. Both the quantity and quality of the information on risks and controls developed to date by your external auditors will vary widely depending on the firm you use, the budget pressure you have applied, and the integrity and competence of the individual audit partner assigned to your account.
5. Concentrate initial formal risk and control assessment work on DOPs that are considered to be of high importance to your external disclosures and/or have demonstrated a historical pattern of error/variability. Take steps to identify the major risks and “significant controls” that are used to mitigate those risks. The

March 2003 AICPA exposure draft "REPORTING ON AN ENTITY'S INTERNAL CONTROL OVER FINANCIAL REPORTING" states: *"The practitioner should evaluate the design and operating effectiveness of significant controls for each of the components of internal control and for each significant account balance, class of transactions, and disclosure and related assertions."* Over time, coverage will have to be expanded to include all significant DOPs to meet the needs of your external auditor for section 404 assertions.

6. To keep external audit review work and fees to a minimum, if the risk and control assessments have been prepared by work unit personnel or a special risk and control documentation team, consider having your internal audit group or an outsourced equivalent, evaluate the process used to perform the disclosure risk and control assessment and complete any substantive testing considered necessary to determine if the control status representations are reliable. Attachment 2 overviews a range of different traditional direct report and self-assessment assurance strategies that can be used to support control representations. Attachment 8 provides an overview of a structured 6 level quality assurance framework that can be used to quality assure SOX control status/deficiency representations generated by work units and/or management personnel. The willingness of external auditors to rely on quality assurance work done by internal audit staff at this point is unclear. External auditing standards related to section 404 audit opinions have not been finalized by the Public Company Accounting Oversight Board as of April 2003. The draft AICPA guidance in the area states *"The practitioner should **not** rely on the results of internal auditor procedures as the principal evidence of the operating effectiveness of controls over significant accounts, classes of transactions, and disclosures. However, the practitioner may consider such work in determining the nature, timing, and extent of his or her testing"* (page 18 of 45, Reporting on an Entity's Internal Control Over Financial Reporting, issued in draft by the AICPA in March 2003).
7. To meet section SOX section 302 requirements for reliable quarterly representations, DOP primary owners/sponsors should update process variability/error rates and input any new information on risks that threaten the DOPs and/or the controls in use to mitigate those risks each quarter. The status of any action plans to address concerns should also be updated. This activity needs to be documented and a trail maintained in the system to provide evidence of a quarterly review required by section 302.
8. Identify DOPs and Disclosure Staging Areas that exhibit significant variability/error and/or have significant residual risks. Under SOX section 302(a)(5) "significant deficiencies" need to be reported upwards to your audit committee and your external auditor together with documentation of any corrective actions underway. Any "significant deficiencies" identified should be reviewed by the CEO and CFO responsible for signing the required 302/404 quarterly and annual control representations. This step should be done prior to

reporting these issues to the external auditor and audit committee. Some companies have also created a Disclosure Review Committee for this purpose. Evidence that this review has occurred should be documented and kept on file.

9. Your external auditor will need to evaluate the Disclosure Staging Area and DOP process variability/error rates and the impact of any “significant deficiencies” identified internally to determine their impact, if any, on their opinion on the management control representation required by SOX section 404. They will also need to consider the impact, if any, of the control deficiencies on their opinion on the financial statements.

RECOMMENDATION #3 – THE SOX 302/404 MINIMALIST APPROACH – USE IT AT YOUR OWN RISK

If your organization is not sold on the business case for the type of approach outlined in Recommendations #1 and #2, you will likely gravitate to the “Minimalist Approach”. The ramifications of opting for a minimalist approach on your company’s ability to attract qualified audit committee members, the Corporate Governance Score (“CGS”) assigned to your company by rating agencies and any related implications of your CGS on your cost of capital, implications on your ability to obtain cost effective Director and Officer insurance, the likely reactions of any regulators that oversee your business sector, and other factors should all be considered.

To execute this approach you need to confer with your external auditor to determine the bare minimum amount of work they will accept to provide you with a sign-off on your assertion. Until specific auditing standards for SOX section 404 attestations are finalized and released by Public Company Accounting Oversight Board (PCAOB), external auditors will be only able to provide “best guesses” of their actual requirements. They will also have to carefully assess the implications of the Minimalist Approach on their legal liability.

It is expected that at least some of the external audit firms will accept approaches significantly less rigorous than those suggested in Recommendation #1 and #2.

It is expected that finalized audit standards for audit opinions on management control representations will be issued over the next few months. Subject to the feedback you get from your external auditor, you will then need to negotiate the optimal combination of internal and external assessment work to keep your external audit fee to an acceptable level and still obtain a positive section 404 audit report.

CAUTIONS TO CONSIDER

CAUTION #1 – CONTROL ASSESSMENT TEMPLATES PROVIDED BY YOUR EXTERNAL AUDITOR

If you are considering using a SOX section 302/404 control assessment template/software developed by your external audit firm, check with your legal counsel to get an opinion on whether this would violate any independence rules established by SOX and/or the SEC. Since a pre-populated control assessment template makes assumptions about what are, and are not, key controls, and explicitly or implicitly makes assumptions about the likelihood and consequence of various risks, this may preclude the external audit firm from rendering an objective opinion on a senior management control representation. If you have the misfortune to have a serious and very public control disaster after a positive section 404 audit opinion, your external auditor's independence in the control assessment and representation process may be questioned. This could, in a worse case scenario, bring into question whether the external audit opinion on your control representation and/or financial statements had been compromised.

CAUTION #2 – INVOLVEMENT OF YOUR EXTERNAL AUDITOR DEVELOPING YOUR CONTROL REPRESENTATION

If you are considering using your external audit firm to play a role in the development of SOX section 302/404 risk and control documentation, check with your legal counsel to ensure that this will not violate any independence rules. You should also discuss their involvement with your Audit Committee to ensure that they are happy with this external audit service activity. In addition to technical legal issues, you will also need to consider whether outside parties, including any future litigants/plaintiffs, would consider direct involvement of your external auditor in the development of your company's risk and control analysis and control representation an independence problem. You may also wish to check with your Director and Officer ("D&O") and Errors and Omission ("E&O") insurance carrier(s) to determine if the utilization of your external auditor to help assess your risk and control status related to external financial disclosures impacts in any way on your insurance coverages/premiums.

CAUTION #3 – INCREASED LEGAL LIABILITY FROM INCREASED RISK/CONTROL STATUS INFORMATION

While developing the risk and control analysis required to support a SOX section 302/404 representations you may identify situations where very serious concerns and problems exist. In some cases, these problems may have existed and been known by management personnel for some time. These issues may not have been visible and/or documented previously. You should immediately confer with legal counsel to determine the best course of action to deal with issues of this type.

CAUTION #4 – OBSOLESCENCE OF APPROACHES THAT FOCUS ON CONTROL COMPLIANCE AND IGNORE RISK IDENTIFICATION/ASSESSMENT

Some of the older style control assessment methods and tools focus attention almost exclusively on the existence of what are generally known as "Direct controls". Little or no attention is paid in these older methods to documenting end result objectives, identifying and assessing the likely risks to those objectives, and considering the broader range of control types, including such things as commitment controls, capability controls, measurement and oversight controls and others, necessary to manage key risks. Although the 1992 version of COSO did not focus heavily on the critical importance of risk identification and assessment, the new COSO conceptual framework scheduled for release in final in late 2003 significantly elevates and explains the importance of these steps. The adoption of methods and tools that do not explicitly include risk identification and analysis could result in your external auditor denying a positive opinion on your control representation. It is generally expected that the new 2003 COSO conceptual framework will form the primary assessment criteria that will be used by external auditors to form their opinion on CEO and CFO control representations required by SOX section 404.

WHAT THE FUTURE HOLDS

Although history tells us that projecting the future is a difficult task to say the least, my best guesses of SOX 302/404 trends and developments follow:

BEST GUESS #1 - ACCEPTANCE OF QUALITY PRINCIPLES

Financial disclosure regulators will slowly encourage the use of the more "scientific" process assessment approaches that have been promoted by the quality movement for many decades. This will eventually require companies to measure and report process variability/error rates in the processes that support external disclosures to senior management, audit committees and external auditors.

BEST GUESS #2 - ELEVATION OF THE IMPORTANCE OF RISK ASSESSMENT

The importance on identifying outcomes required from disclosure systems and identifying and assessing risks to those outcomes will become mandatory as the newest generation of the COSO framework is released in 2003, and the global movement to adopt Enterprise Risk Management accelerates.

BEST GUESS #3 - IMPROVED AUDIT QUALITY

SOX section 404 will force internal and external auditors to focus more attention on the reliability of the processes that support external disclosures. This emphasis should, assuming efforts to restore independence to external auditor/company relationships succeed, result in a lower incidence of, and less material, external auditor failures.

BEST GUESS #4 - PLAINTIFFS AND REGULATORS WILL EXPLOIT HOLES IN "QUICK FIX" SOX COMPLIANCE PROGRAMS

SOX 302/404 has now, to a much greater degree, codified U.S. corporate risk and control governance expectations. In cases where a company has the misfortune of having a material external disclosure misstatement, the amount of effort the company has expended to comply with sections 302 and 404 will play a key role in determining plaintiff and regulator damages and punishments.

BEST GUESS #5 - INCREASED USE OF WORK UNIT RISK & CONTROL SELF-ASSESSMENT ("RCSA")

The new requirements for quarterly monitoring of all DOPs and Disclosure Staging Areas will provide an incentive for companies that have historically relied on traditional "direct report" assessment approaches done by internal audit and compliance personnel to adopt, to a much greater extent, risk and control self-assessment.

SOX Sections 302 & 404: Full Text

SEC. 302. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS.

(a) REGULATIONS REQUIRED. — The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that —

(1) the signing officer has reviewed the report;

(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;

(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;

(4) the signing officers:

(A) are responsible for establishing and maintaining internal controls;

(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

(C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and

(D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function) —

(A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and

(B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

(b) **FOREIGN REINCORPORATIONS HAVE NO EFFECT.** — Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.

(c) **DEADLINE.** — The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act.

SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

- (a) **RULES REQUIRED.** — The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall —
- (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
 - (2) contain 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.
- (b) **INTERNAL CONTROL EVALUATION AND REPORTING.** — With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

SOX Assurance Strategies - Options Overview

DIRECT REVIEW & REPORT BY ASSURANCE SPECIALISTS	MACRO OBJECTIVE: Ensure SEC disclosures, including the financial statements, notes to the financial statements, and applicable supplemental disclosures, are complete, timely and reliable.			SELF-ASSESSMENT BY RESPONSIBLE WORK UNIT(S)
DRR#1 COMPLIANCE FOCUS Assurance Specialists review and report on conformance with rules/policies/audit questionnaires.	Disclosure Staging Area			SA#1 COMPLIANCE FOCUS Work units self-assess their state of compliance and prepare a report on conformance with rules/policies.
DRR #2 PROCESS FOCUS Assurance Specialists examine business process(es) and provide opinions/ observations on adequacy/effectiveness/status of the process(es).	Revenue/Sales Accounting	Property Plant & Equipment	Litigation Disclosures	SA#2 PROCESS FOCUS Work units self-assess business process(es) and report opinions/ observations on adequacy/effectiveness/ status.
DRR #3 OBJECTIVE FOCUS Assurance Specialists select one or more end result objective(s) for assessment and provide opinions on adequacy/ effectiveness/risk status.	Invoice Payment Accounting	Accounts Receivable Collection/Valuation	Contingent Liability Identification/Disclosure	SA#3 OBJECTIVE FOCUS Work units select one or more end result objective(s) for assessment and report opinions/observations on adequacy/effectiveness.
DRR #4 RISK FOCUS Assurance Specialists select a context such as business unit, process, or objective(s) and identify and rank the risks and assess the effectiveness of the controls currently in place to mitigate them.	Payroll & Benefits	Related Party Transactions	Executive Equity Activity	SA#4 RISK FOCUS Work units select one or more objectives and identify and rank the risks or threats to that context, rate the likely effectiveness of controls currently in place to mitigate them, and provide a report on residual risk status.
DRR #5 CONTROL FRAMEWORK FOCUS Assurance Specialists review the macro level control framework used to manage the area/topic selected using the assessment criteria in one or more management control model (e.g. COSO, CoCo, CARD® model).	Inventory Accounting/Valuation	Investment Accounting	Guarantees & Warranties	SA#5 CONTROL FRAMEWORK FOCUS Work units review the macro level framework used to manage the area/ topic selected against the criteria in one or more control frameworks.
PRODUCT: REPORT FROM THE ASSURANCE SPECIALIST PROVIDING OPINIONS/ OBSERVATIONS ON CURRENT ADEQUACY OR EFFECTIVENESS OF COMPONENT REVIEWED.	Short & Long Term Debt Accounting	Federal/State Income Tax	Deferred Tax Accounting	ASSURANCE SPECIALISTS PERFORM A QUALITY ASSURANCE REVIEW ON THE SELF-ASSESSMENT PROCESS AND/OR REPRESENTATIONS AND REPORT ON THE RELIABILITY.
	Share Register/ Stock Option Activity	Intangible Asset Accounting	Pension Fund Accounting	
	Research & Development Activity/Accounting	Derivatives/Hedging Activities	Risks the Company Faces	
	Foreign Exchange Accounting	Acquisitions/ Divestitures	Business Segment Disclosure	

Basel Bank Governance Deficiencies Summary

Summary of Deficiencies in Risk/Control/Assurance Management Identified By the Basle Committee on Banking Supervision *(Note: Based on our global experiences, the deficiencies identified are common to all organizations, both public and private sector)*

1. Board of Directors and senior management did not establish strong control cultures.
2. Senior management failed to emphasize the importance of a strong control culture through their words and actions and, most importantly, through the criteria used to determine compensation and promotion.
3. Senior management failed to ensure that the organization structure and management accountabilities were well defined.
4. Senior management weakened the control culture by promoting and rewarding managers who were successfully generating profits but failed to implement control policies or address audit findings.
5. Accountabilities were not clearly defined.
6. Inadequate risk recognition and assessment processes.
7. Some banks failed to observe certain key internal control principles especially segregation of duties.
8. Senior management did not respond appropriately to information they were receiving.
9. High-level reviews were not being done. Situations that should have been flagged as abnormalities were not investigated by senior management.
10. Information was not reliable or complete and communication was not effective.
11. Banks failed to adequately communicate employee's duties and control responsibilities or disseminated policies through channels, such as electronic mail, that did not ensure that the policy was read, understood and retained.
12. Lines of communication did not exist for the reporting of suspected improprieties by employees.
13. Banks did not effectively monitor their risk/control systems. The systems did not have the necessary built-in ongoing monitoring processes and the separate evaluations performed were either not adequate or were not acted upon appropriately by management.
14. There was a failure to consider and react to day-to-day information provided to line management and other personnel indicating unusual activity.
15. Failure to react to situations indicating a heightened level of risk.

Summary of Deficiencies in Risk/Control/Assurance Management Identified By the Basle Committee on Banking Supervision *(Note: Based on our global experiences, the deficiencies identified are common to all organizations, both public and private sector)*

16. Internal audit was not effective in many problem banking organizations. This was caused by piecemeal audits, lack of a thorough understanding of business processes, and inadequate follow-up when problems were noted.
17. Fragmented audit approaches resulted because the internal audits were structured as a series of discrete audits of specific activities within the same division or department, within geographic areas, or within legal entities.
18. Inadequate knowledge and training of internal audit staff in trading products and markets, electronic information systems, and other highly sophisticated areas.
19. Internal audit staff were hesitant to ask questions when they suspected problems, and when questions were asked, they were more likely to accept an answer than to challenge it.
20. Management did not accept the role and importance of internal audit and did not appropriately follow-up on issues identified.
21. Senior management failed to receive timely and regular tracking reports that indicated critical issues and the subsequent corrective actions taken by management.

Source: Supervisory Lessons Learned from Internal Control Failures, Appendix II, Framework for Internal Control Systems in Banking Organizations, Basle Committee on Banking Supervision, Basle, September 1998. (www.bis.org/publ/bcbs40.htm)

Basel Committee on Banking Supervision
Sound Practices for the Management and Supervision
of Operational Risk
February 2003

Developing an Appropriate Risk Management Environment

Principle 1: The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

Principle 2: The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.

Risk Management: Identification, Assessment, Monitoring and Mitigation/Control

Principle 4: Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

Principle 5: Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

Principle 6: Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Role of Supervisors

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

Role of Disclosure

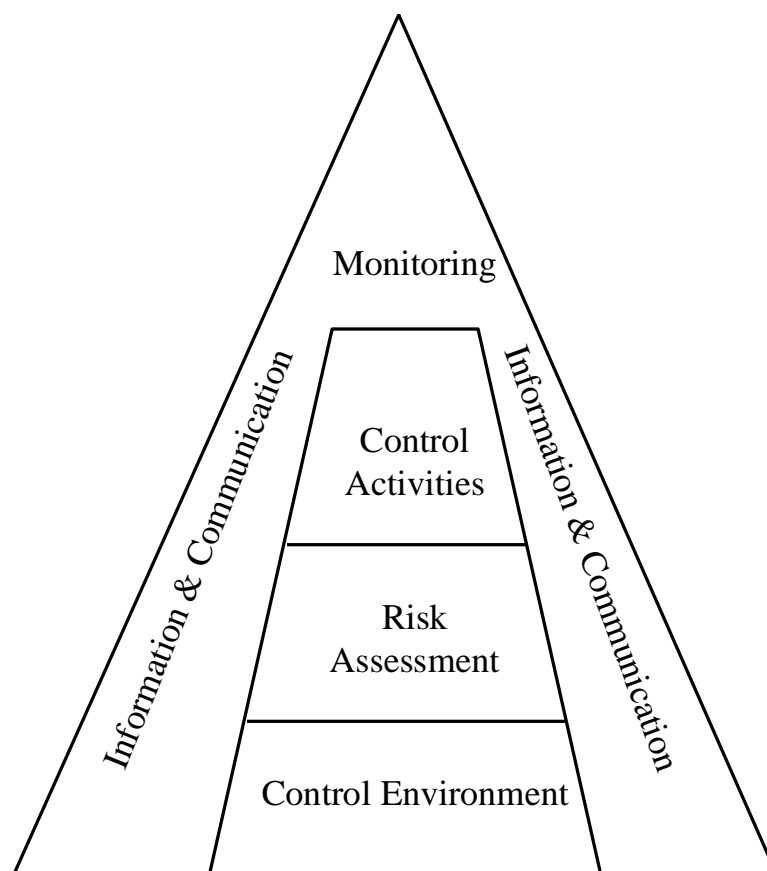
Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

Source: Basel Committee, Bank for International Settlements, Sound Practices for the Management and Supervision of Operational Risk, February 2003, www.bis.org/publ/bcbs96.htm

Control Models

COSO FINAL SEPTEMBER 1992

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.

COSO 1992 (U.S.)

<p>1. CONTROL ENVIRONMENT</p> <p>1.1 Integrity and Ethical Values 1.2 Commitment to Competence 1.3 Board of Directors/Audit Committee 1.4 Management Philosophy and Operating Style 1.5 Organization Structure 1.6 Assignment of Authority and Responsibility 1.7 Human Resource Policies and Practices</p> <p>2. RISK ASSESSMENT</p> <p>2.1 Entity-Wide Objectives 2.2 Activity-Level Objectives 2.3 Risk Identification 2.4 Change Management</p> <p>3. CONTROL ACTIVITIES</p> <p>3.1 Top Level Reviews 3.2 Direct Functional or Activity Management 3.3 Information Processing 3.4 Physical Controls</p>	<p>3. CONTROL ACTIVITIES (CONT'D)</p> <p>3.5 Performance Indicators 3.6 Segregation of Duties 3.7 Controls Over Information Systems</p> <ul style="list-style-type: none">• Data Centre• Application Development & Maintenance• System Software• Access Security• Application Controls <p>4. INFORMATION AND COMMUNICATION</p> <p>4.1 Information 4.2 Communication</p> <p>5. MONITORING</p> <p>5.1 Ongoing Monitoring 5.2 Separate Evaluations 5.3 Reporting Deficiencies</p>
--	---

NOTE:

The subpoints noted under each category heading are derived from the narrative in the COSO Framework volume. COSO does not attempt to list specific subelements in the framework for each category but does provide detailed criteria for each category posed as questions.

COSO Enterprise Risk Management Conceptual Framework - Expected April 2003

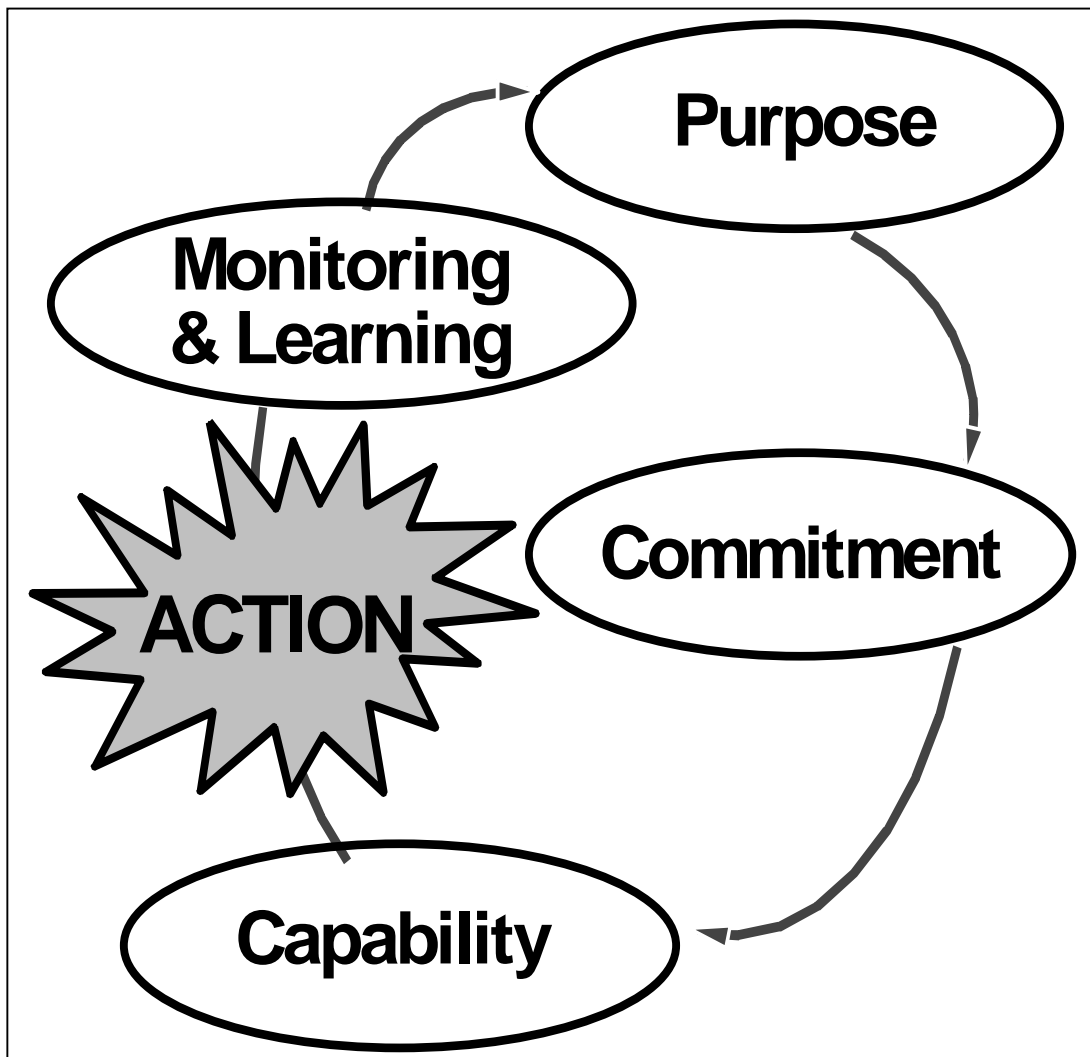
Conceptual Framework - Key Concepts

1. Internal Environment
2. Event Identification
3. Risk Assessment
4. Risk Response
5. Control Activities
6. Information and Communication
7. Monitoring
8. Limitations
9. Roles and Responsibilities

Draft Enterprise Risk Management definition

..... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise designed to identify and manage potential events that may affect the entity and to provide reasonable assurance regarding the achievement of entity objectives.

SOURCE: COSO presentation, GAM Conference Orlando, Florida, March 2003



Reproduced with permission from the Canadian Institute of Chartered Accountants.

CoCo SEPTEMBER 1995 IN CANADA

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.

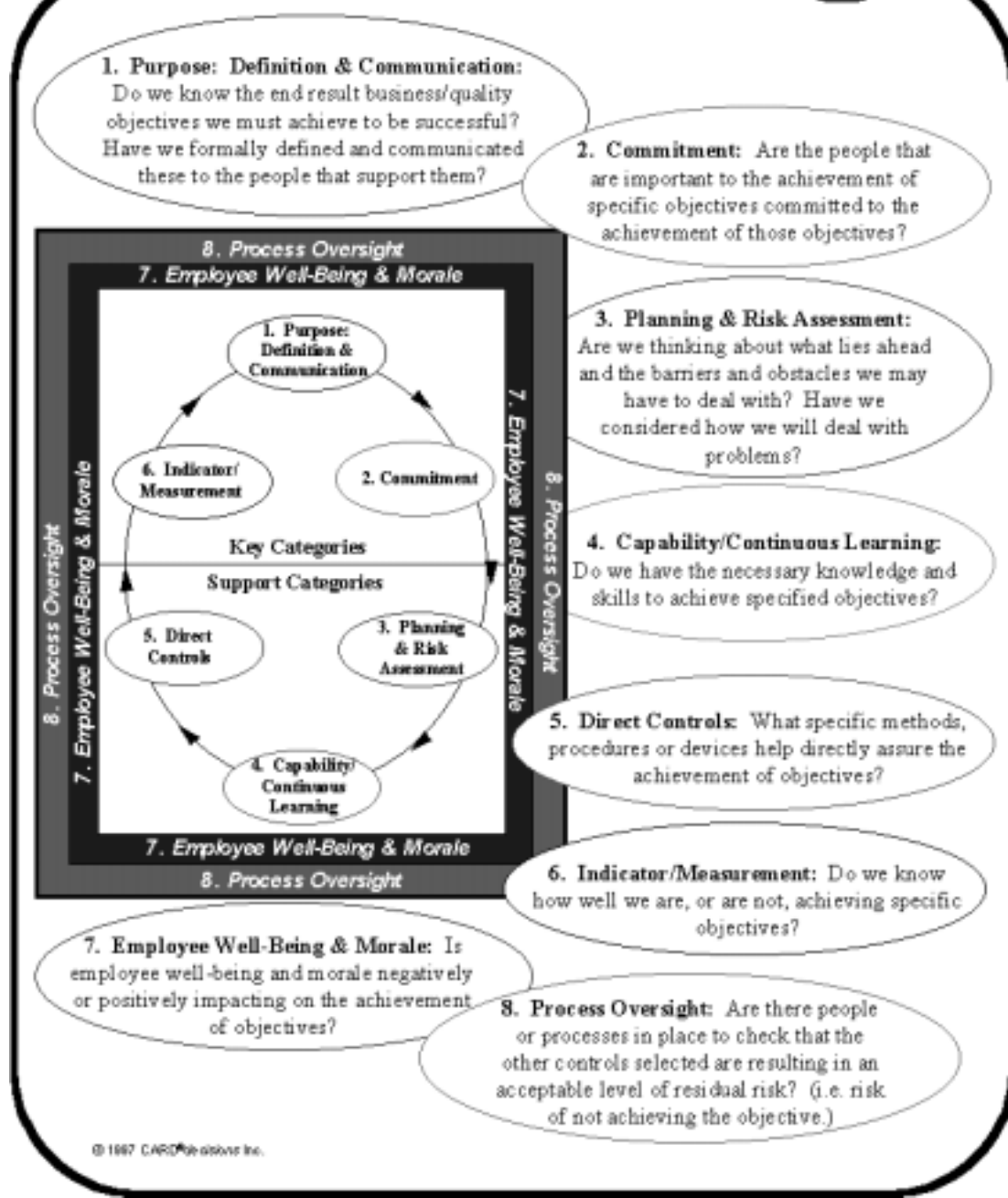
CAPABILITY

- 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.

CARD[®]model



NOTE: The first version of this control framework was developed in 1986 at Gulf Canada Resources. It has undergone numerous revisions over the years based on feedback from internal and external auditors, work unit personnel and senior management around the world. The next version release is scheduled for May 2003. This framework and the sub-elements shown on the next page are "Freeware" and are available for use by the general public with attribution to CARD[®]decisions. CARD[®]model is acknowledged as a practical and leading international framework in IIA publications "Control Self-Assessment: A Practical Guide", pages 34 and 35 and "Implementing the Professional Practices Framework", pages 141 to 143.

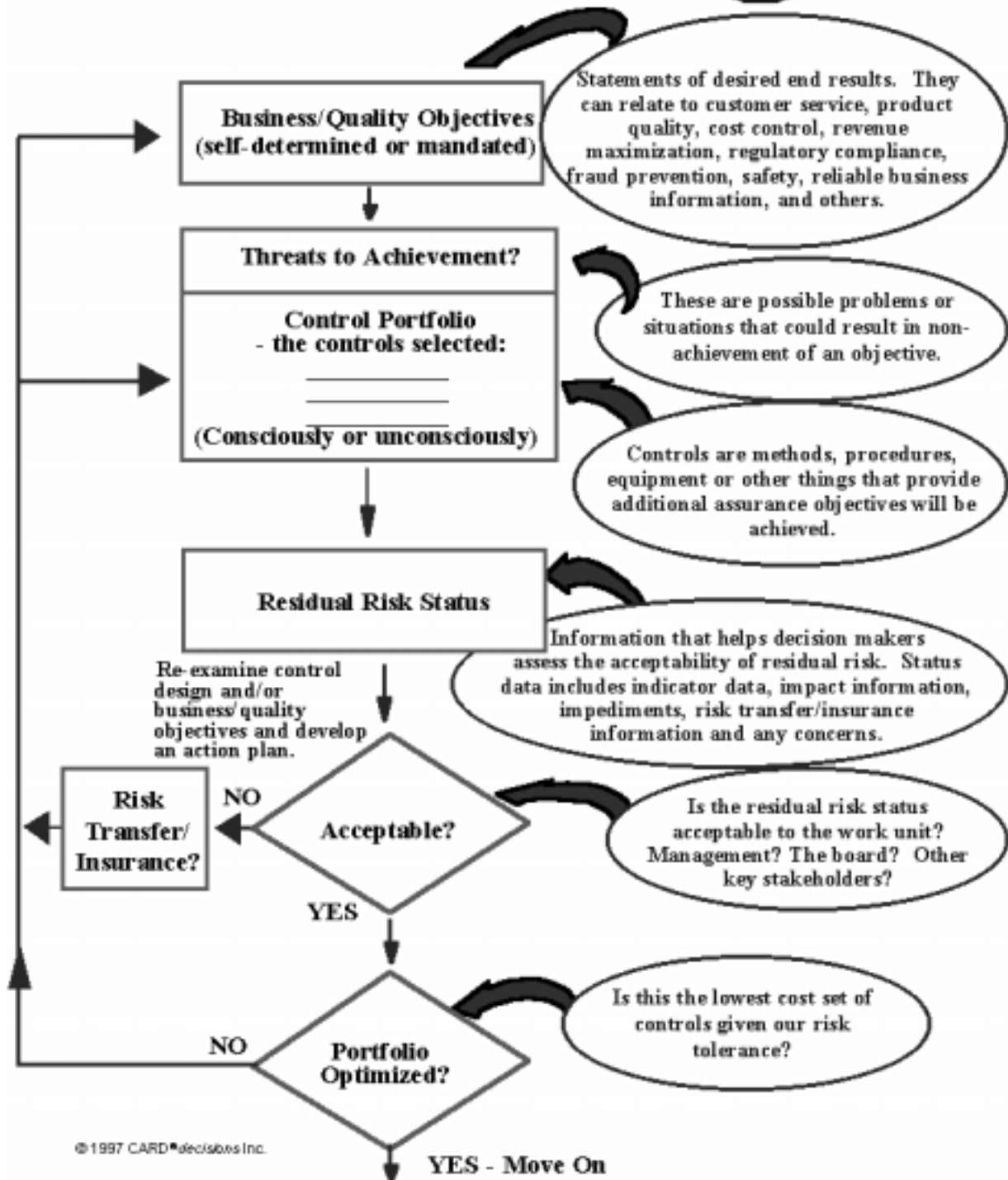
- | | |
|---|---|
| <p>1. PURPOSE: DEFINITION & COMMUNICATION</p> <p>1.1 Definition of Corporate Mission & Vision</p> <p>1.2 Definition of Entity Wide Objectives</p> <p>1.3 Definition of Unit Level Objectives</p> <p>1.4 Definition of Activity Level Objectives</p> <p>1.5 Communication of Business/Quality Objectives</p> <p>1.6 Definition and Communication of Corporate Conduct Values and Standards</p> <p>2. COMMITMENT</p> <p>2.1 Accountability/Responsibility Mechanisms</p> <p>2.1a Job Descriptions</p> <p>2.1b Performance Contracts/Evaluation Criteria</p> <p>2.1c Budgeting/Forecasting Processing</p> <p>2.1d Written Accountability Acknowledgements</p> <p>2.1e Other Accountability/Responsibility Mechanisms</p> <p>2.2 Motivation/Reward/Punishment Mechanisms</p> <p>2.2a Performance Evaluation System</p> <p>2.2b Promotion Practices</p> <p>2.2c Firing and Discipline Practices</p> <p>2.2d Reward Systems - Monetary</p> <p>2.2e Reward Systems - Non-Monetary</p> <p>2.3 Organization Design</p> <p>2.4 Self-Assessment/Risk Acceptance Processes</p> <p>2.5 Officer/Board Level Review</p> <p>2.6 Other Commitment Controls</p> <p>3. PLANNING & RISK ASSESSMENT</p> <p>3.1 Strategic Business Analysis</p> <p>3.2 Short, Medium and Long Range Planning</p> <p>3.3 Risk Assessment Processes - Macro Level</p> <p>3.4 Risk Assessment Processes - Micro Level</p> <p>3.5 Control & Risk Self-Assessment</p> <p>3.6 Continuous Improvement & Analysis Tools</p> <p>3.7 Systems Development Methodologies</p> <p>3.8 Disaster Recovery/Contingency Planning</p> <p>3.9 Other Planning & Risk Assessment Processes</p> <p>4. CAPABILITY/CONTINUOUS LEARNING</p> <p>4.1 Knowledge/Skills Gap Identification and Resolution Tools/Processes</p> <p>4.2 Self-Assessment Forums & Tools</p> <p>4.3 Coaching/Training Activities & Processes</p> <p>4.4 Hiring and Selection Procedures</p> <p>4.5 Performance Evaluation</p> <p>4.6 Career Planning Processes</p> <p>4.7 Firing Practices</p> <p>4.8 Reference Aids</p> <p>4.9 Other Training/Education Methods</p> | <p>5. DIRECT CONTROLS</p> <p>5.1 Direct Controls Related to Business Systems</p> <p>5.2 Physical Safeguarding Mechanisms</p> <p>5.3 Reconciliations/Comparisons/Edits</p> <p>5.4 Validity/Existence Tests</p> <p>5.5 Restricted Access</p> <p>5.6 Form/Equipment Design</p> <p>5.7 Segregation of Duties</p> <p>5.8 Code of Accounts Structure</p> <p>5.9 Other Direct Control Methods, Procedures, or Things</p> <p>6. INDICATOR/MEASUREMENT</p> <p>6.1 Results & Status Reports/Reviews</p> <p>6.2 Analysis: Statistical/Financial/Competitive</p> <p>6.3 Self-Assessments/Direct Report Audits</p> <p>6.4 Benchmarking Tools/Processes</p> <p>6.5 Customer Survey Tools/Processes</p> <p>6.6 Automated Monitoring/Reporting Mechanisms & Reports</p> <p>6.7 Integrity Concerns Reporting Mechanisms</p> <p>6.8 Employee/Supervisor Observation</p> <p>6.9 Other Indicator/Measurement Controls</p> <p>7. EMPLOYEE WELL-BEING & MORALE</p> <p>7.1 Employee Surveys</p> <p>7.2 Employee Focus Groups</p> <p>7.3 Employee Question/Answer Vehicles</p> <p>7.4 Management Communication Processes</p> <p>7.5 Personal and Career Planning</p> <p>7.6 Diversity Training/Recognition</p> <p>7.7 Equity Analysis Processes</p> <p>7.8 Measurement Tools/Processes</p> <p>7.9 Other Well-Being/Morale Processes</p> <p>8. PROCESS OVERSIGHT</p> <p>8.1 Manager/Officer Monitoring/Supervision</p> <p>8.2 Internal Audits</p> <p>8.3 External Audits</p> <p>8.4 Specialist Reviews & Audits</p> <p>8.5 ISO Review/Regulator Inspections</p> <p>8.6 Audit Committee/Board Oversight</p> <p>8.7 Self-Assessment Quality Assurance Reviews</p> <p>8.8 Authority Grids/Structures & Procedures</p> <p>8.9 Other Process Oversight Activities</p> |
|---|---|

Risk Source Models







AS/NZS 4360: 1999 D2	AS/NZS 4360: 1999 D5
<ol style="list-style-type: none"> 1. Commercial and legal relationships 2. Economic circumstances 3. Human behaviour 4. Natural events 5. Political circumstances 6. Technology and technical issues 7. Management activities and controls 8. Individual activities 	<ol style="list-style-type: none"> 1. Diseases 2. Economic 3. Environmental 4. Financial 5. Human 6. Natural hazards 7. Occupational health and safety 8. Product liability 9. Professional liability 10. Property damage 11. Public liability 12. Security 13. Technological






CARD[®] decisions Risk Source Framework	
<ol style="list-style-type: none"> 1. Commercial/Legal 2. Competition 3. Control Design 4. Customers 5. Employees 6. Environmental Liability 7. Equipment/Technology 8. Finance/Economic 	<ol style="list-style-type: none"> 9. Fraud/Corruption 10. Human Behaviour 11. Missing Objectives 12. Natural Events 13. Political Influences 14. Product/Service Liability 15. Public Perception 16. Suppliers

CARDline



Risk Management Capability Assessment Criteria

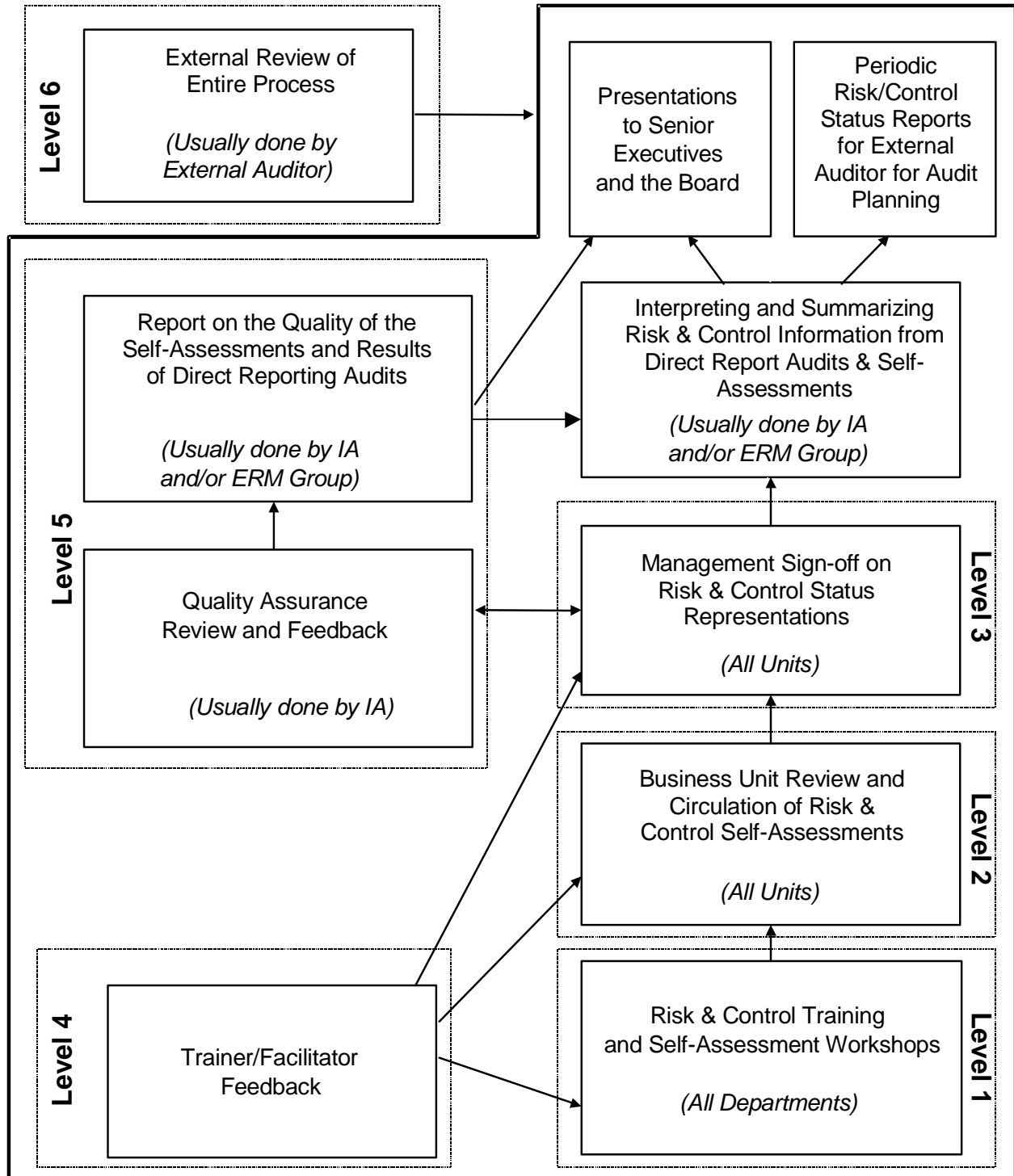
<p>1. Risk Assessment</p> <p>How do you identify and measure the threats/risks that could impact on the achievement of your business objectives?</p>	<p>SCORE:</p> <div style="border: 1px solid black; padding: 5px; width: 40px; margin: 0 auto;">  </div>
<p>2. Control Assessment</p> <p>How healthy are your control frameworks? How long has it been since you evaluated their effectiveness?</p>	<p>SCORE:</p> <div style="border: 1px solid black; padding: 5px; width: 40px; margin: 0 auto;">  </div>
<p>3. Control Cost Optimization</p> <p>Could you eliminate some controls and still have an acceptable residual risk level at a lower overall cost?</p>	<p>SCORE:</p> <div style="border: 1px solid black; padding: 5px; width: 40px; margin: 0 auto;">  </div>
<p>4. Risk Testing the Future</p> <p>Do you consider and evaluate risks when making important business decisions and preparing strategic plans?</p>	<p>SCORE:</p> <div style="border: 1px solid black; padding: 5px; width: 40px; margin: 0 auto;">  </div>
<p>5. Planning for Serious Risk Situations</p> <p>Do you have contingency plans in place to deal with low probability, high risk situations that could cripple your unit or the company? Do you periodically revisit these plans to reassess their adequacy?</p>	<p>SCORE:</p> <div style="border: 1px solid black; padding: 5px; width: 40px; margin: 0 auto;">  </div>
<p>6. Worst Case Scenarios</p> <p>Have you considered the possibility of high risk situations which, if they occurred together, could have a devastating effect on the company?</p>	<p>SCORE:</p> <div style="border: 1px solid black; padding: 5px; width: 40px; margin: 0 auto;">  </div>

<p>7. Early Warning Systems</p> <p>Do you regularly monitor your risk status for early warning signs that changes are needed to your controls and/or objectives?</p>	<p>SCORE:</p> <p></p>
<p>8. Risk Transfer/Financing Options</p> <p>Have you considered risk transfer and insurance options available to avoid or reduce the consequences of specific threats/risks to your business objectives?</p>	<p>SCORE:</p> <p></p>
<p>9. Regular Reevaluation</p> <p>Do you periodically reassess the acceptability of your risk acceptance decisions?</p>	<p>SCORE:</p> <p></p>
<p>10. Oversight Process</p> <p>Does Senior Management and the Board of Directors understand the major risks the company faces and take steps to ensure work units are identifying, measuring, controlling and monitoring risks?</p>	<p>SCORE:</p> <p></p>
<p style="text-align: right;">TOTAL RISK FITNESS SCORE: </p>	

Note: This CARD[®] *decisions* risk management evaluation tool is recognized as an emerging best practice tool in the IIA publication "Implementing the Professional Practices Framework" on page 126. The new IIA professional standards require Internal Auditors evaluate their company's risk management system. On page 100 the IIA Professional Standards Guide states:

The new Implementation Standard 2110 A1 makes it clear internal auditors should review the risk management system as part of their assurance activities for the board and senior management. This represents new territory for most internal audit shops. Few organizations have established processes for assuring the adequacy and effectiveness of risk management procedures.

SOX 302/404 Quality Assurance Strategies



Sarbanes-Oxley Key Result Areas Regarding Risk & Control

1. Ensure senior management and the Board are provided with timely and reliable information on the state of risk and control to meet SOX sections 302 and 404.
2. Ensure the company's external auditor is provided with reliable information on the state of risk and control and, specifically, the level of variability/error in the processes that support external accounting disclosures.

6 Quality Assurance Levels That Provide Assurance That Self-Assessment Representations Are Reliable

Level 1 Quality Assurance - During the Workshop From the Group and the Facilitator

Level 2 Quality Assurance - During the Business Unit's Review of Results Developed in Self-Assessment Workshops

Level 3 Quality Assurance - During the Consensus Sign-off of Self-Assessment Results by Work Unit Senior Management

Level 4 Quality Assurance - Through Feedback on Quality From the Self-Assessment Trainers/Facilitators

Level 5 Quality Assurance - Through an Independent Review Including Testing of the Self-Assessment representations and the Feedback/Reporting/Coaching Process (usually done by Internal Audit)

Level 6 Quality Assurance - Through an Independent Review of the Entire Risk & Control Assessment and Reporting Process done by the Company's External Auditor.

Sample Management Representation to Audit Committee

We, the undersigned, acknowledge to the Audit Committee 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 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 you, 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

What's Wrong with the Status Quo? - Detailed Comments

1. CORPORATE SECTOR RESISTANCE TO CONTROL REPRESENTATIONS

Proposals have been made by the SEC since 1979 calling for representations on the reliability of control systems from senior management with a report to stakeholders on the reliability of management's assessment from their external auditors. These proposals were routinely defeated as a result of the significant power of various lobby groups in the U.S. A central argument against the proposed representation requirements was that the business community was taking steps to reform and additional regulatory burden was unnecessary, and/or the Foreign Corrupt Practices Act was already doing the job. Unfortunately, it is my observation that many of these lobby groups were far more interested in entrenched self-interests than maintaining the confidence of the investment community and long-term viability of capital markets. It is unfortunate that necessary changes to corporate governance regimes have had to be imposed on the business community by regulators, instead of being self generated by internal and external professional institutes. A central tenant of being a professional is to place the interests of your client ahead of your personal interests. There appears to have been widespread confusion in the internal and external audit professions on who is their primary client.

2. OPINING ON WHETHER CONTROL IS "ADEQUATE"

Colossal and recurring external auditor failures around the world regularly demonstrate the difficulty of providing opinions on the reliability of financial statements. Positive audit opinions are regularly issued on materially false financial disclosures in spite of the fact that the U.S. has developed thousands of pages of rules on how they should be prepared to "fairly" present the company's financial status. The difficulty of providing an opinion or an assertion that internal control is "adequate" or "effective" to ensure the reliability of external financial disclosures is exponentially greater. There are very few guidelines to help auditors decide when there are "adequate" internal controls. Field research done by CARD[®] *decisions* with hundreds of groups of senior level internal audit and management personnel has consistently demonstrated that, given the exact same circumstances in a case situation, few groups and few individuals in those groups agree on the combination of control elements from a predetermined control design menu that would provide an "effective" or "adequate" level of control. This is true

in spite of the fact that internal audit departments around the world routinely give opinions to clients on whether the clients' internal controls are "adequate". It takes very little applied research to demonstrate conclusively that audit opinions on what constitutes an "adequate" level of control involve a huge amount of highly subjective judgment. These findings suggest that reporting these highly subjective opinions on whether controls are "adequate" or "effective" to key stakeholders does not meet the goals of comparability, reliability, and repeatability, key criteria for sound assurance and audit methods.

3. INABILITY OF EXISTING CONTROL ASSESSMENT TOOLS TO PREDICT DISASTER

In hundreds, if not thousands of cases, internal auditors around the world have reported to senior management and audit committees that controls in a company or sub-unit of a company are "adequate" or "effective". Massive control failures, some causing the complete demise of major companies, have occurred in organizations shortly after positive assurance reports were delivered. Few, if any, attempts have been made by the Institute of Internal Auditors or American Institute of Certified Public Accountants, or any other professional or research group I am aware of to study why the internal risk and control assessment approaches and tools used by auditors in these organizations failed to identify and predict these massive failures. There is no empirical evidence at this point that the auditor opinion success rate is any higher in companies where the auditors use control criteria to form their opinions, such as COSO, the U.S. control model, or CoCo the Canadian control model, than those companies where auditors making "modelless" control status representations and/or opinions.

4. LIMITED COVERAGE OF THE TOTAL RISK UNIVERSE

The majority of formal, documented risk and control assessment work has historically been prepared by auditors and/or external consultants. This analysis usually only covers a small fraction of the total universe of end result financial statement objectives and processes in any given year, let alone, each quarter. Very few organizations today can demonstrate that they have documented the risks, controls and process variability related to all key processes that feed the Disclosure Staging Area shown on page 6. Even fewer companies have demonstrable and reliable self-assessment regimes in place to ensure that these processes are being monitored on a quarterly basis to determine if they are producing reliable product to feed the Disclosure Staging Area - a key requirement of SOX sections 302 and 404.

5. NOT LOOKING IN THE RIGHT PLACES

As a general statement, internal auditors have historically done very little work to assess the quality of controls in the Disclosure Staging Area shown on page 6. This is true in spite of the fact that history tells us that many of the biggest financial reporting failures in history occurred in the Disclosure Staging Area. Primary reasons cited by Internal Auditors for not focusing assessment efforts on this area are that it would overlap with work done by the External Auditor, they lack staff with current knowledge of Generally Accepted Accounting Principles ("GAAP") and SEC disclosure rules, and/or they have been told by the CFO not to examine the processes used to produce external disclosures. In many companies, the head of Internal Audit reports to the CFO. Examining and reporting problems in the Disclosure Staging Area would mean reporting deficiencies in processes owned and/or controlled by the CFO and, in some severe cases, ethics/integrity problems related to the activities of their boss (e.g. Enron, WorldCom, HealthSouth, etc). It doesn't take a genius to know that reporting your boss is "Integrity Challenged/A Crook" would be a CLM – a Career Limiting Move.

6. NO REWARDS FOR DISCLOSING THE TRUTH

The SOX requirement that there must be a process in place to report significant deficiencies in internal control upwards to external auditors and the audit committee is generally inconsistent with the culture of "catch me if you can" that has evolved in many companies. There are few rewards in most companies for work units that tell internal or external auditors problems they are aware of with the current reliability of risk and control management processes. Major culture changes are usually necessary to encourage work units to report bad news. In many companies these culture changes have not occurred. In case after case of major corporate reporting failures, the Board of Directors, CEO and CFO are claiming they didn't know what was going on. Over the course of my career I have heard more than one U.S. Chief Legal Counsel state categorically, "There is no way we want the CEO and/or Board knowing about those problems". The Richard Nixon "plausible deniability" principle is still a cornerstone in more than a few companies as a result of direct advice from their legal advisors. In cases where the CEO, CFO and Board genuinely didn't know what was going on in their companies, this was virtually assured by the design of the corporate reward/business systems they established.

7. EXTERNAL AUDIT METHODOLOGIES

In the late 70s when I was training to be an external auditor with Coopers & Lybrand we were taught that we must evaluate controls over the key processes that contribute to the financial statements. This activity had to be documented with interview and flowcharts. We had to identify the "key controls" in those processes, the controls essential to ensuring the reliability of the information being produced, for testing and evaluation. As time went by, the emphasis placed by external audit

firms on documenting and evaluating the control environment and processes that feed the financial statements, and the training costs, time, and fees that it required, came under heavy pressure from clients that wanted lower external audit fees. The goal of many companies was to get the cheapest possible signature on the financial statements that could be obtained from a major accounting firm with a globally recognized name (i.e. the "cheapest possible signature"). To accomplish this, the major external audit firms moved to approaches that placed more emphasis on testing of balance sheet balances and analysis of financial ratios and less emphasis on attempting to evaluate the likely reliability of the processes and control environment that produce the numbers. This transition away from formal, documented risk and control evaluation occurred in spite of the fact that the complexity of the business environments, and the dependency on computer systems that create the numbers in external disclosures, increased exponentially. Many new external auditors trained in the 1990s received only limited training on how to formally assess risks and controls in the business processes that support the many financial statement disclosure line items and supplemental disclosures. Little effort appears to have been expended anywhere in the world to empirically study the specific external audit methods in use today to critically gauge their predictive ability (i.e. back test failures to examine the reliability of vulnerability analysis done by external auditors during the planning stage). Access to the information necessary to complete this type of study would likely be blocked or severely restricted by legal advisors of external audit firms concerned with litigation exposure unless there was strong regulatory support for such a study.

8. INTERNAL AND EXTERNAL AUDITORS, STANDARD SETTERS, AND REGULATORS IGNORE BREAKTHROUGHS IN QUALITY MANAGEMENT

Over the past 20 years major advances have been made in the area of process quality control and assurance. Frameworks such as ISO 9000, Malcolm Baldrige and Six Sigma teach people to focus on process reliability and reducing process variability and error. The focus in these systems is on identifying and controlling process variability and driving down error and rework. Although financial disclosures are nothing more than the sum of the reliability of dozens of sub-processes, the tremendous advances in quality thinking have been largely ignored by the key players involved in seeking and providing assurance on external financial disclosures, and the professional bodies and regulators who oversee these activities. The Basel Capital Accord reforms in the banking sector constitute the first signs of hope in this area. The Sarbanes-Oxley legislation does not appear to explicitly recognize these quality principles.

9. INTERNAL AND EXTERNAL AUDITORS, STANDARD SETTERS AND REGULATORS IGNORE BREAKTHROUGHS IN RISK MANAGEMENT

In 1995 the Australian/New Zealand Standard on Risk Management [AS/NZS 4360], was released. It is credited with playing a key role in shifting the emphasis from a focus on controls compliance to a focus on management of risks

to business objectives and/or processes. The core elements of risk management are shown in Attachment 6 to this paper. A central element of the risk management movement is that assessments should start with seeking clarity on the outcome(s) sought, examine risks that threaten the achievement of the outcome(s) and then, and only then, examine the existence and quality of "Risk Treatment", the selection and implementation of appropriate control options for dealing with risk. Although the Basel bank governance reforms have clearly recognized that a risk focus is far superior to a fixation on controls compliance (see Attachment 3 page 3), there is very little recognition in SOX that the emphasis should be on evaluating and reporting on the quality of an organization's risk identification, measurement and mitigation strategies related to reliable financial disclosures. While some might argue that evaluating the "adequacy" of internal controls implicitly considers, and must include, evaluating the risks and the objectives to be achieved, there are important and significant differences.

10. **INDIFFERENT AND NON DISCRIMINATING CUSTOMERS**

Over the years I have worked with hundreds of large companies all over the world on risk and assurance assignments. In more than a few of these companies, senior management and audit committees showed very little interest in understanding and critically evaluating the quality of the assurance products and services delivered by internal and external auditors. High quality assurance products and services often received the exact same reaction from senior executives and Audit Committees as extremely poor quality assurance products and services. After observing this disconcerting phenomenon in scores of major listed public companies, I can only conclude that the senior management and audit committees in those companies either didn't care what they received in the way of assurance products or services, and/or couldn't recognize a good product and service from a bad one. Indifferent customers do not drive continuous improvement and promote the evolution of high quality assurance products and services

Contrasting Traditional Assurance Strategies and ERAM

<u>Historical/Traditional</u>	<u>The New Vision</u>
<ul style="list-style-type: none"> • Assign Duties/Supervise Staff • Policy/Rule Driven • Limited Employee Participation and Training • Narrow Stakeholder Focus • Auditors and Other Specialists are the Primary Control Analysts/Reporters 	<ul style="list-style-type: none"> • Empowered/Accountable Employees • Continuous Improvement/learning Culture • Extensive Employee Participation and Training • Broad Stakeholder Focus • Staff at all levels, in all functions, are the Primary Control Analysts/Reporters
MANAGEMENT AND STAFF - HISTORICAL/TRADITIONAL	MANAGEMENT AND STAFF - THE NEW VISION
<ul style="list-style-type: none"> • Are responsible for complying with prescribed methods and procedures. • Receive limited training on control and quality assessment and design. • Often consider auditors, consultants, and other specialists to be the experts on control and quality systems and design. • Outside specialists are often called in to analyze areas where concerns and/or problems exist. • Are often not allowed or encouraged at lower levels to analyze and make decisions relating to risk acceptance or control design. • The personnel doing the work are often not directly responsible for selecting the controls used that help assure that their business/quality objectives are achieved. • Candidness and full disclosure on the current state of control and risk is not encouraged and is often discouraged and punished. • Fear and blame are sometimes utilized as strategies when problems surface. • Internal control and total quality/continuous improvement are not integrated programs or concepts. 	<ul style="list-style-type: none"> • Are accountable for designing and maintaining control systems that provide the desired level of assurance regarding the achievement of business/quality objectives. • Are provided with adequate risk and control assessment and design skills to properly fulfill their responsibility to report to Officers, the Board, and others on the current status of control, quality and risk. • Consensus at all levels on relevant business/quality objectives and levels of acceptable risk is a primary goal. • Candid disclosure of the state of control and the risks being accepted by the unit/organization is encouraged and rewarded. • Accountability for business/quality objectives exists and is accepted by staff at all levels, in all functions. • Employees at all levels are responsible for finding new and better ways to improve and optimize control portfolios to better achieve key business/quality objectives. • Employees at all levels and in all functions continually reassess the adequacy and appropriateness of control choices and make adjustments when new information emerges regarding risk status, prioritization of objectives, and the control options available. • Control and quality management are considered to be synonymous terms and are fully integrated programs/concepts.

Contrasting Traditional Assurance Strategies and ERAM

<u>Historical/Traditional</u>	<u>The New Vision</u>
<ul style="list-style-type: none"> • Assign Duties/Supervise Staff • Policy/Rule Driven • Limited Employee Participation and Training • Narrow Stakeholder Focus • Auditors and Other Specialists are the Primary Control Analysts/Reporters 	<ul style="list-style-type: none"> • Empowered/Accountable Employees • Continuous Improvement/Learning Culture • Extensive Employee Participation and Training • Broad Stakeholder Focus • Staff at all levels, in all functions, are the Primary Control Analysts Reporters
AUDIT - HISTORICAL/TRADITIONAL	AUDIT - THE NEW VISION
<ul style="list-style-type: none"> • A primary objective is to perform audits and report findings to senior management, and/or external stakeholders. • Relations with auditees are sometimes adversarial. • Auditors are viewed as the control "experts". Control assessment training is directed primarily to auditors and staff specialists. • A primary audit objective is to report on whether units are complying with prescribed controls, procedures and standards. • How auditors decide what constitutes "effective" or "adequate" control frameworks. How much risk is considered acceptable is often not explicitly disclosed. • Auditors are measured primarily on execution of prescribed audit and review processes. • Auditors receive limited training on risk and control design concepts and ways to "optimize" control frameworks. • Internal auditors rarely examine and report on control frameworks related to customer service, product/service quality, safety, environmental compliance, and other "non-financial" areas. • Quality auditors rarely examine or report on regulatory compliance, corporate ethics, fraud prevention and detection or the reliability of management representations to the Board and/or external stakeholders. 	<ul style="list-style-type: none"> • Primary audit objectives are to: <ul style="list-style-type: none"> - raise the risk and control assessment and design skills of all staff; - provide accurate and complete information to the Officers, the Board and external stakeholders on the state of risk and control management systems; - assist staff at all levels to design and maintain better, more optimal risk and control management frameworks. • A key audit role is to foster more effective risk and control management through training, coaching, facilitation, and feedback to staff - unless quality assurance reviews suggest that representations by work units are misleading and the "good faith" assumption is not appropriate. • Auditors help to ensure that the organization's business/quality objectives recognize a range of stakeholders, including customers and regulators, and that operative objectives are consistent with the corporate mission/vision. • Auditors are measured on, and accountable for, achievement of the primary objectives noted above, not on excellent execution of traditional audit processes (i.e. focus on results not activity execution). • Auditors should be skilled and knowledgeable risk and control design analysts and excellent technical auditors. These skills should extend to customer service, product quality, environmental compliance, fraud prevention and detection, and safety, as well as traditional financial reporting objectives.