INTERNAL CONTROL

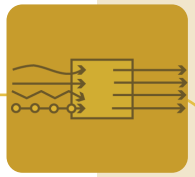
COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices

PARVEEN P. GUPTA, LLB, PH.D.
LEHIGH UNIVERSITY

Published by
Institute of Management Accountants
10 Paragon Drive
Montvale, NJ 07645-1760
www.imanet.org

IMA INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

CMA CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™



INTERNAL CONTROL

COSO 1992 Control Framework and Management Reporting on Internal Control: Survey and Analysis of Implementation Practices

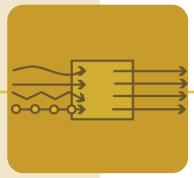
Parveen P. Gupta, LLB, Ph.D.
Frank L. Magee Distinguished Professor of Accounting

College of Business and Economics
Rauch Business Center #37
Lehigh University
Bethlehem, PA 18015
610.758.3443
ppg0@lehigh.edu

IMA INSTITUTE OF MANAGEMENT ACCOUNTANTS
Advancing the Profession™

CMA CERTIFIED MANAGEMENT ACCOUNTANT
Professionals Driving Business Performance™

ENTERPRISE RISK AND CONTROL



ENTERPRISE RISK AND CONTROL

"We are particularly eager to hear whether there are actions that we can take to improve the internal control documentation, assessment, reporting, and auditing processes. For example, the PCAOB's Auditing Standard Number 2 gives guidance to independent external auditors tasked with determining whether a company's internal controls are effective. No similar guide, however, exists for companies and for their management. And in the absence of direction from us, companies have been basing the assessment of their controls on AS-2. Management and auditors clearly have different duties and responsibilities. Wouldn't management benefit from having guidance from the Securities and Exchange Commission on what constitutes adequate controls?"

—Opening Remarks of the SEC Chairman,
Honorable Christopher Cox,
at the SEC/PCAOB Roundtable
on Second-Year Experiences
with Internal Control
Reporting Requirements.
Washington, D.C., May 10, 2006.[1]

1 Transcript of Discussion as posted on www.sec.gov.
See p. 7, Lines 7–20.

Published by Institute of Management Accountants, 10 Paragon Drive, Montvale, NJ, 07645-1760, www.imanet.org

COSO 1992 CONTROL FRAMEWORK AND MANAGEMENT REPORTING ON INTERNAL CONTROL OVER FINANCIAL REPORTING: SURVEY AND ANALYSIS OF IMPLEMENTATION PRACTICES

TABLE OF CONTENTS

ABOUT THE AUTHOR

Parveen P. Gupta is the Frank L. Magee Distinguished Professor of Accounting at the College of Business and Economics at Lehigh University. He received his Ph.D. from Pennsylvania State University in 1987 and an MBA with dual concentration in accounting and finance from the University of Connecticut in 1983. Parveen also holds a law degree from University of Delhi in India. Since joining Lehigh University in 1987, Parveen has developed and taught undergraduate, graduate, and executive education courses in ethics, corporate governance, business risk management, internal control, internal auditing, balance scorecard, total quality management, and business process reengineering. In 2000 and 2003, Parveen was selected by his graduate students as the Outstanding MBA Professor of the Year. During 2005 Parveen received a national award from the American Accounting Association for his curriculum innovation in the area of ethics, corporate governance, risk, and control.

Parveen's research focuses on investigation of corporate governance practices on financial disclosures and firm performance, impact of enterprise-wide risk management on a firm's cost of capital, information content of control deficiency reporting under the Sarbanes-Oxley Act of 2002 and capital market's reaction to such disclosures in terms of impact on a firm's stock price, bid-ask spread etc., audit quality and performance evaluation practices within large CPA firms, communications with the audit committee, control and coordination processes within professional audit organizations, and implementation of quality and reengineering within the internal audit and finance functions in business organizations. His research has been published in major academic and practitioner journals like *Administrative Science Quarterly, American Sociological Review, Accounting, Organization and Society, Organization Studies, International Journal of Accounting, International Journal of Disclosure and Governance, Accounting Enquiries, Internal Auditor, Managerial Auditing Journal, and Journal of Accountancy*. His research has been funded by the American Accounting Association, Financial Executives Research Foundation, Institute of Internal Auditors Research Foundation and the Institute of Management Accountants. He has published two major research monographs in the area of internal auditing. His most recent research has focused on internal control certifications under Sections 302 and 404 of the Sarbanes-Oxley Act of 2002. One of his recent research studies in this area titled *Control Deficiency Reporting: Review and Analysis of Filings During 2004* was published by Financial Executives Research Foundation in 2005. He is also the co-author of a book titled *Sarbanes-Oxley: A Practical Guide to Implementation Challenges and Global Response* published by Risk Books in 2006.

Parveen has also been recognized for his research accomplishments by the Association of Chartered Accountants in the U.S. through a Best Research Paper Award and Lehigh University's Beidleman Research Award. In addition to presenting his research at numerous academic and professional conferences both at a national and international level, Parveen has appeared on CNNfn's "Maverick of the Morning" show and is often quoted in various media publications including the *Wall Street Journal,* Dow Jones Marketwatch.com, Knowledgeleader.com, CFO.com, *The Morning Call,*

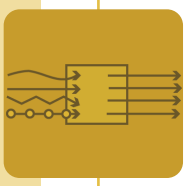
ABOUT THE AUTHOR

Democrat & Chronicle, Christian Science Monitor, Compliance Week, CFO Magazine, and *Treasury & Risk*.

Parveen's work and consulting experience is across a broad spectrum of accounting, management, and business areas. During the last 15 years, he has advised numerous *Fortune* 500 companies and Big 4 public accounting firms. Parveen currently serves as a Research Fellow with the Enterprise Risk Management Initiative of North Carolina State University. He is either currently serving or has served in the recent past as a member of the editorial board of the *Internal Auditor*, *Journal of International Accounting and Taxation*, Canadian Institute of Chartered Accountants' Risk Management and Governance Board, American Accounting Association's Professionalism and Ethics Committee, National Association of Corporate Directors Philadelphia Chapter's Program Advisory Board, and the Institute of Internal Auditor's Professional Issues Committee and International Quality Committee. Besides being inducted into the Beta Gamma Sigma and Beta Alpha Psi business and accounting honor societies, Parveen is also an active participant in the Financial Executives International (FEI), Institute of Internal Auditors (IIA), American Accounting Association (AAA), Institute of Management Accountants (IMA), and the National Association of Corporate Directors (NACD).

ABOUT IMA®

With a worldwide network of nearly 65,000 professionals, IMA is the world's leading organization dedicated to empowering accounting and finance professionals to drive business performance. IMA provides a dynamic forum for professionals to advance their careers through Certified Management Accountant (CMA®) certification, research, professional education, networking, and advocacy of the highest ethical and professional standards.



ACKNOWLEDGEMENTS

This research study would not have been possible without the guidance and participation of many individuals and organizations. First and foremost, I would like to thank the Institute of Management Accountants for providing me with the necessary funding to undertake this research project. I am particularly grateful to Jeffrey C. Thomson, vice president of research and applications development at the Institute of Management Accountants, for working with me patiently and providing me with all the flexibility and guidance throughout the survey development and distribution, data collection, analysis, and writing of this research study.

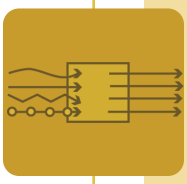
I am also very grateful to Brenda Lovell and Margie Poposky, both of the Institute of Internal Auditors, for helping me with the distribution of the survey to their membership. Inclusion of internal auditors' responses has provided much needed data for richer analysis of critical issues explored in this study. Special thanks also go to Paul Sharman, president and CEO of the Institute of Management Accountants, and Dave Richards, president and CEO of the Institute of Internal Auditors, for allowing me to include a cover letter, on their behalf, in the survey in my efforts to solicit a higher response rate from the IMA and IIA members.

Thanks are also due to the following members of the Research Advisory and Review Board for providing me with valuable feedback and critique during the writing phase of the research study: Tim Leech, Bruce McCuaig, Sandra B. Richtermeyer, Steven J. Root, William G. Shenkir, Mark C. Southon, Patrick J. Stroh, Jeffrey C. Thomson, Betsy Socci, and Michael Zanoni.

Throughout the survey development phase numerous individuals provided me with their valuable time and perspective by pilot testing several versions of the survey instrument to ensure that the survey consists of managerially relevant questions of current importance. I owe the most debt of gratitude to all survey participants who took the time out to complete the 20-page survey and also shared their insights and thoughts through a number of "write-in" comments. There is no way I would have been able to complete this research study without their input and commitment to completing the survey. I also thank many individuals who provided me with their insights either through various telephone or face-to-face interviews during all aspects of this research study.

Last but not least, I would also like to thank Kathy Williams, *Strategic Finance* editor, Maureen Walsh, IMA's director of marketing, and Ann Freestone, freelance editor, for their editing, layout, and publication assistance.

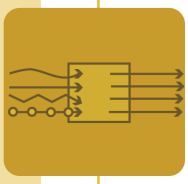
—Parveen P. Gupta



EXECUTIVE SUMMARY

The Sarbanes-Oxley Act of 2002 was signed into law by President Bush on July 30, 2002, in the wake of corporate scandals of Enron and WorldCom to restore investor confidence in the U.S. capital markets. The law charged the U.S. Securities and Exchange Commission (SEC) with implementing its various provisions under a strict timeline and as a result of past audit failures disenfranchised the auditing industry from self-regulation by creating the Public Company Accounting Oversight Board (PCAOB). Since the enactment of the far-reaching governance reforms mandated by the Sarbanes-Oxley Act, Section 404 has consistently dominated the headlines and created an unprecedented amount of backlash as well as counterpoint expressions of support from all those affected by its new internal control certification requirements. Central to the new internal control certifications under Section 404 is the requirement that management and auditors assess the effectiveness of a company's system of internal control over financial reporting in accordance with a "suitable" internal control framework. According to the Section 404 SEC Final Rules and the PCAOB's Auditing Standard No. 2 (AS2), the Internal Control—Integrated Framework (also known as COSO 1992 to distinguish it from COSO's other two products, ERM and Small Business Guidance) developed and issued by the Committee of the Sponsoring Organizations of the Treadway Commission (COSO) meets the stated suitability criteria and can be relied upon both by management and the external auditors for conducting internal control effectiveness evaluations under Section 404 of the Sarbanes-Oxley Act.

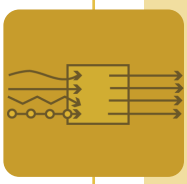
Since the passage of the Sarbanes-Oxley Act, a number of surveys and research studies have been conducted on the costs and benefits of implementing the Section 404 management and auditor certification requirements. The majority of these studies have focused on analyzing the extensive costs flowing from these new compliance requirements. To date, however, none of these surveys and research studies has examined how companies and their external auditors are, in fact, using the COSO 1992 Framework to assess and report on the effectiveness of a company's internal control over financial reporting. This research study fills this void by documenting the current implementation practices at the SEC registrants as they pertain to the use of the COSO 1992 Framework within the context of Section 404 control effectiveness reporting requirements. It analyzes the responses of the 374 participants from firms of varying sizes. Additionally, the motivation for this research study also comes from the fact that the COSO 1992 Framework was developed at a time when formal opinions and certifications on the effectiveness of a company's internal control over financial reporting were not mandatory. No systematic research has yet been conducted that validates the robustness of this control model in an environment where companies and auditors are required to unequivocally conclude whether an SEC registrant has an effective or ineffective system of internal control over financial reporting. Thus, the findings of this research study contribute important information for public policy decisions by the appropriate regulatory bodies and the standard setters around the world as they assess the practicality and viability of these new rules in the U.S. and other countries. This research study analyzes the survey responses of a large cross-section of the SEC registrants on a number of Section 404 certification-related issues, including the application of integrated external audit, meaning and use of the top-down/risk-based assessment approach,



skills required to effectively conduct internal control effectiveness evaluations, relevance and extent of use of the guidance provided in each of the five components of the COSO 1992 Framework for conducting fraud-risk assessments, and IT control evaluations, determining what constitutes "key controls" and identification of the appropriate amount of related documentation and testing to conclude on the effectiveness of internal controls, determination of "material weaknesses" and related remediation plans, and other contentious areas of these new regulations.

Overall, the implications of this research study's findings are that the COSO 1992 Framework provides a principles-based model to understand and think about internal controls in an organization but falls short of providing implementation guidance that would significantly help management conduct a top-down/risk-based integrated assessment of internal controls over financial reporting in a sustainable and cost-effective manner. The survey respondents also indicated that they did not rely significantly on the guidance provided by the COSO 1992 Framework to conduct the required fraud vulnerability risk assessments, IT control evaluations, identification of what constitutes "key controls," and determining limits on documentation and testing to conclude when their system of internal control over financial reporting is effective and, most importantly, how management and auditors should address the fundamental question of how much and what kinds of controls are required to assure the reliability of the external audit opinions on financial statements issued to the public.

Some of the public policy implications of this study's findings are that the COSO Board (1) should reevaluate the suitability of the COSO 1992 Framework in light of the new demands placed on it to meet the Section 404 requirements; (2) should carefully and objectively assess whether the reliance on the current guidance by management to assess and report on controls is as efficient and effective as possible to minimize the "unintended" consequences associated with Sections 302/404 certifications, including the excessive compliance costs being incurred and the significant erosion in the position of the United States as the preeminent global capital market. In addition, those COSO organizations that are involved in education and certification-related activities should jointly sponsor a project that would focus on identifying the most significant skill gaps that exist currently in the management, external audit, and internal audit communities with the goal of proposing practical steps that should be taken jointly to close this gap as soon as possible to ensure the continued success of the control governance reforms so appropriately put in place by the Sarbanes-Oxley Act of 2002.



I. INTRODUCTION

On July 30, 2006, it was four long years since the passage of the Sarbanes-Oxley Act of 2002[2] (hereinafter referred to as SOX)—the landmark legislation that has irrevocably changed the way U.S.-listed corporations (small or large) view and approach corporate financial reporting and related disclosures. When signing the unanimously passed bill into law, President Bush applauded it by declaring:

> This new law sends very clear messages that all concerned must heed....[It] says...to every dishonest corporate leader: You will be exposed and punished; the era of low standards and false profits is over; no boardroom in America is above or beyond the law...to corporate accountants: The high standards of your profession will be enforced without exception; the auditors will be audited; the accountants will be held to account...to shareholders that the financial information that you receive from a company will be true and reliable, for those who deliberately sign their names to deception will be punished.[3]

No doubt, these were strong words. They continue to reverberate through stricter enforcement, disciplinary actions, lawsuits, and fines imposed by regulatory agencies in charge of implementing the law. When passing the law in the shortest timeframe in the recent legislative history of the United States, Congress clearly wanted to restore investor confidence in the U.S. capital markets by combating fraudulent financial reporting, conflicted investment banking and auditing practices, egregious executive behavior, and by holding boards of directors to higher standards of control governance oversight.

The message was loud and clear. All companies, whether domestic or foreign, wanting to raise capital in the U.S. equity or debt markets will have to adhere to higher corporate governance standards imposed by SOX. Although "most executives wondered why they should be subjected to the same compliance burdens as those who had been negligent or dishonest,"[4] the U.S. capital markets were generally euphoric, and countries around the globe began to consider whether they should also follow suit by enacting similar reforms to their capital markets. Unfortunately, this honeymoon was short-lived. Although SOX was passed in the right spirit as an antidote to the widespread corporate malfeasance represented by poster-child companies like Enron, WorldCom, HealthSouth, Qwest Communications, Global Crossing, Adelphia Communications, Tyco, etc., unfortunately, its enforcement has been marred by a whole host of implementation challenges[5] to the extent that now some even want to overturn the legislation completely, and others wish to exempt more than 75% of all publicly traded companies from one or more of its requirements on the grounds that compliance with SOX is hurting U.S. global competitiveness.

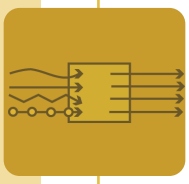
Among other provisions, Section 404 of the Act—calling for internal control effectiveness certifications from management as well as external auditors—is the leading cause of dissention among the regulators, registrants, auditors, and the investing community at large. Auditing Standard No. 2 (hereinafter referred to as AS2) issued by the Public Company

2 Also known as the Public Company Accounting Reform and Investor Protection Act of 2002.

3 White House Press Release. "President Bush Signs Corporate Corruption Bill." July 30, 2002.

4 Wagner, Stephen, and Lee Dittmar. "The Unexpected Benefits of Sarbanes-Oxley." *Harvard Business Review*. April 2006, pp. 133-140.

5 For more discussion on implementation challenges, see Chan, Sally, Parveen Gupta, and Tim Leech. *Sarbanes-Oxley: A Practical Guide to Implementation Challenges and Global Response*. London, England: Risk Books, 2006.



Accounting Oversight Board (PCAOB) is the primary vehicle that that has been used to implement this crucial section of the Act. AS2 requires that management and external auditors conduct their internal control assessments over financial reporting in accordance with an SEC-acceptable internal control assessment framework. According to the SEC Final Rules, the *Internal Control—Integrated Framework*[6] issued in 1992 by the Committee of the Sponsoring Organizations of the Treadway Commission (hereinafter referred to as the COSO 1992 Framework) satisfies the SEC criteria for an acceptable internal control assessment framework.[7]

According to the recently issued Exposure Draft of the Advisory Committee on Smaller Public Companies, the COSO 1992 Framework "has emerged as the only internal control framework available in the U.S. and the framework used by virtually all U.S. companies."[8] The Advisory Committee later in the same exposure draft questions the applicability, sufficiency, and relevancy of the guidance provided in the COSO 1992 Framework in guiding small company managements while conducting internal control assessments over financial reporting. We have heard similar concerns during our field interviews from larger companies. Thus, the purpose of this research study is to explore the extent to which public companies are, in fact, successfully utilizing the guidance provided in the COSO 1992 Framework to comply with the intent and spirit of the Section 404 requirements. Additionally, this research will also explore what, if any, implementation challenges, including skill-set or training, etc., the company managements are encountering while conducting their internal control assessments over financial reporting. The majority of the research conducted to date, as discussed in the next section, has focused on documenting outcomes, consequences, and impacts on companies of all sizes while complying with the internal control certification requirements. None of these surveys and research studies have focused on identifying the root causes of the implementation challenges but rather have focused on quantifying the massive costs incurred by the companies in complying with the Section 404 requirements.

The remainder of this research study is organized in five sections. Section II reviews the background and current status of the SOX 302/404 implementation debate to provide necessary background and context. The key question debated in this section is why well-intentioned internal control certification requirements have become a major political hot potato threatening the nullification of the entire SOX statute. Section III discusses the survey development process and the research methodology. Section IV describes sample statistics including respondent and company demographics to provide appropriate context for understanding the survey's findings. Section V presents the survey results and discusses in detail the findings with implications for practice. Section VI concludes the study with final thoughts.

6 Committee of the Sponsoring Organizations of the Treadway Commission. *Internal Control—Integrated Framework.* Jersey City, N.J.: American Institute of Certified Public Accountants, September 1992.

7 See Section II.B.3(a) of the SEC Final Rule on "Management's Reports on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," which states, "The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements." Also see paragraph 14 of AS2, which states that "in the United States…[COSO 1992 Framework]…provides a suitable and available framework for purposes of management's assessment."

8 Advisory Committee on Smaller Public Companies. "Exposure Draft of Final Report of Advisory Committee on Smaller Public Companies." Washington, D.C.: March 2006, p. 23.

II. BACKGROUND AND CURRENT STATUS OF SOX 302/404 IMPLEMENTATION

There are many provisions in the law that irks Corporate America, but the most notorious are Sections 302 and 404. Collectively these two sections require, for the first time, that (1) the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) of a company certify that financial information presented in their company's 10K and 10Q filings is true and fair, and (2) the management and their external auditors assess and publicly report in a registrant's periodic filings to the SEC whether the company has an effective system of internal control over its financial reporting. This assessment is of paramount importance because, according to Section 404, the existence of even a single material control weakness precludes a registrant as well as its external auditors from concluding that the company has effective internal control over its financial reporting.

II.1. The Rationale

The logic behind these requirements is quite sensible and difficult to refute. The requirements attempt to recognize that "financial statements produced from effective risk and control management systems are more reliable than those that [are] produced in the absence of such systems."[9] Implicit in this notion is the assumption that external auditors of a company are better equipped to provide reliable audit opinions if they have better information on the true state of internal control and related risks. Although the granularity of the debate around SOX often causes the true focus of producing more reliable audit opinions to be obscured, we believe the true intent of the Congress in passing SOX legislation, ceteris paribus, was to minimize the incidence of materially wrong external audit opinions.

On the surface no one disagrees or disputes that the quality of the external audit opinions in the recent past has been questionable and that better internal controls produce more reliable financial disclosures. Even prior to the enactment of SOX, however, company managements were more than willing to state that they own the internal control system that produces their company's financial disclosures. Unfortunately, it is the requirement in Section 404 that "management provide a written opinion on control effectiveness and produce documented support for their internal control effectiveness claims, and, most significantly, that the company's external auditors render their own opinion on internal control over financial reporting and on management's representation on control that has created unprecedented"[10] amount of opposition and backlash from Corporate America, including various interest groups representing small and large companies alike.

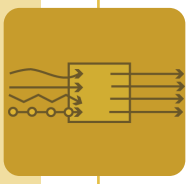
II.2. The Resistance

With every passing year, the calls to modify, alter, or even repeal the internal control requirements in SOX are growing stronger. Most recently, *Financial Times* reported that Alan Greenspan, the former chair of the U.S. Federal Reserve Bank, in a speech given to the delegates attending the Asian Financial Centers Conference said that he believes that the United States would make changes to the SOX legislation, especially to the provisions mandating internal control certifications.[11] Elliot Spitzer, the current attorney general of the state

9 Chan, Sally, Parveen Gupta, and Tim Leech. *Sarbanes-Oxley: A Practical Guide to Implementation Challenges and Global Response.* London, England: Risk Books, 2006, p. 114.

10 Chan, et al., p. 1.

11 "Greenspan Predicts U.S. Governance Revamp." *Financial Times*. April 13, 2006, p. 1.



of New York, who has vigorously pursued corporate wrongdoing under that state's Martin Act, has also come to the same conclusion.[12]

The SEC, being caught between the proverbial rock and a hard place has responded by repeatedly delaying the effective date of implementing the internal control certification requirements imposed by Section 404. Consequently, as of March 15, 2006, only the accelerated filers have become subject to the Section 404 requirements.[13] The nonaccelerated filers[14] (i.e., smaller publicly traded companies) have until after July 15, 2007, to file their first management certification on internal control. The foreign private issuers, accelerated and nonaccelerated, will be phasing in respectively on July 15, 2006, and July 15, 2007.[15]

Although a large number of U.S.-listed corporations (80% by some estimates) have yet to comply with the internal control certification requirements, the resentment to Section 404 requirements has grown to a point where those opposing these requirements have resorted to legal maneuverings by filing a lawsuit on tertiary matters[16] and pinning their hopes of exempting themselves from Section 404 on technical grounds. Contrary to expectations, these groups make no secret of their real intentions. Although the lawsuit filed by the Free Enterprise Fund against the PCAOB allegedly challenges the constitutionality of the appointments to the PCAOB, it is clear that their underlying motive is not to really quibble over the "appointments clause" of the U.S. Constitution but really is to "spur the courts and Congress to undo the entire Sarbanes-Oxley Act."[17] Unlike most other statutes passed by Congress, the SOX law does not contain a severability provision which, in essence, allows Congress to amend part of the act without really opening up the whole legislation[18] and subjecting it to a completely new vote.

Prior to this frontal attack on SOX, many groups have been covertly or overtly lobbying against the reforms imposed by SOX and seeking exemptive relief on behalf of their constituents.

12 "Spitzer Says Sarbanes-Oxley Rules Go Too Far." www.reuters.com. March 14, 2006.

13 See Final Rule Release Nos. 33-8392, 34-49313, and IC-26357 issued by the Securities and Exchange Commission.

14 See SEC Final rule 33-8128. According to the press release 2005-134 dated September 21, 2005, an accelerated filer is a company that has at least $75 million but less than $700 million in public float. Companies with more than $700 million in public float are now called large accelerated filers, and companies with less than $75 million in public float are designated as small accelerated filers.

15 See Final Rule Release Nos. 33-8618 and 34-52492 issued by the Securities and Exchange Commission.

16 See Free Enterprise Fund v. The Public Company Accounting Oversight Board, case No. 1:06CV00217 (U.S. District Court for the District of Columbia, February 7, 2006). According to the article "Is PCAOB Unconstitutional?" published in *The New York Law Journal* by John C. Coffee, Jr., the plaintiffs, represented by Kenneth W. Starr, raise three constitutional objections to the PCAOB: "First, PCAOB allegedly violates the separation of powers doctrine because Sarbanes-Oxley Act purports to insulate it from presidential control by placing the responsibility for its oversight, including the power to remove its members, in a body other than the president (namely, the SEC); Second, because PCAOB's five members are appointed by the SEC (after consultation with specified other federal agencies), this procedure was asserted to violate the Appointments Clause of the U.S. Constitution; [and] finally, PCAOB was challenged as an unconstitutional delegation of 'legislative power to an entity outside the Legislative Branch.'"

17 Katz, David M. "Sarbox Takes a Constitutional." www.CFO.com. February 14, 2006.

18 *Ibid*. According to the article,"while many federal laws have a 'severability' provision that enables Congress to change a section of a law without dismantling it entirely, Sarbanes-Oxley doesn't, according to Michael Carvin, a lawyer with Jones Day in Washington and lead attorney for the plaintiffs."

For example, the American Electronics Association (AeA) representing nearly 3,000 high-tech companies released a report in February 2005 that unequivocally declared "Section 404 of the Sarbanes-Oxley Act (the Act) is having a devastating impact on AeA's small- and medium-sized member companies.... Section 404 implementation is the quintessential example of the *law of unintended consequences* [emphasis added], with the biggest victim being small business."[19] The report concludes with the following list of concerns with the implementation of Section 404 (See page 4):

1. Evidence suggests that the COSO/COBIT frameworks being used to implement Section 404 will not be effective in stopping fraud.
2. The cost serves as a major regressive tax on small and medium companies because the cost is not directly proportional to revenue.
3. The cost of implementation is more than 20 times greater than the SEC estimated in June 2003.
4. The costs will remain very high in years two and three.
5. The expense and bureaucratic mechanism created by Section 404 hurt U.S. competitiveness.
6. Section 404 is pushing a number of smaller companies to go private or consider doing so.
7. Section 404 results in such a huge increase in compliance costs that some foreign companies now are considering withdrawing from U.S. financial markets.

19 "Sarbanes-Oxley Section 404: The 'Section' of Unintended Consequences and Its Impact on Small Business." Washington, D.C.: American Electronic Association, February 2005, p. 1.

The U.S. Chamber of Commerce, a business federation representing companies and business associations, has released many reports criticizing the internal control certification requirements. In one of its most recent reports the Chamber concludes the following: "U.S. markets are the most highly regulated on earth....But how much is too much? At what point does the system become overburdened by rules? Does greater disclosure always result in greater benefit for the investor? Many knowledgeable commentators have asserted that there is no evidence that Section 404 would have done anything to prevent the scandals at Enron and WorldCom. There is beginning to be significant evidence that one small provision of Sarbanes-Oxley Section 404 (168 words out of the several thousand of the act)—may be the tipping point."[20]

Similarly, almost a year earlier, in the comment letter filed with the SEC in response to its call for feedback on first-year implementation experiences with Section 404, the Chamber attacked the internal control certification requirements by stating that it hurt the "long-term competitiveness of U.S. companies and the U.S. capital markets."[21] Consistent with the Chamber's hypothesis, there have been a number of reports in the media[22] indicating that initial public offerings have declined in the U.S. since the passage of SOX and a number of U.S.-listed public companies have been contem-

20 "Capital Markets, Corporate Governance, and the Future of the U.S. Economy." Washington, D.C.: U.S. Chamber of Commerce, February 2006, p. 6.

21 See U.S. Chamber of Commerce comment letter dated April 12, 2005, filed with the SEC in response to its call for first-year implementation experiences with Section 404.

22 See, for example, "Small U.S. Firms take AIM in London," which states that "...drawn by less regulation and lower costs, companies go public in a U.K. market." *Wall Street Journal*, April 17, 2005.

plating going dark due to the excessive compliance burden (in terms of time, cost, and confusion) imposed by the internal control certification requirements. In a recent speech, former chair of the U.S. Federal Reserve Bank, Alan Greenspan, was quoted as saying, "I am nevertheless acutely aware and disturbed by the fact that initial public offerings have moved away from the U.S.—and to a large extent have moved to London."[23]

Besides raising alarms about the macroeconomic impact of the internal control requirements in the same letter, the Chamber has also zeroed-in on a number of root causes that it believes are contributing to the increased compliance burden and consequently lesser competitiveness of U.S. businesses. First, it states that:

> …interpretive guidance should not be left to the auditing firms. Also, in fulfilling its statutory roles under Section 404 and Section 107 of the Act, the SEC should develop guidelines for reporting companies in the implementation of AS2 and the assessment of internal controls in coordination with parallel activities of the PCAOB. (See page 3)

In other words, the Chamber is suggesting that the SEC provide a "practical and generally accepted control assessment criteria that company managements can use to assess and report on the effectiveness of their internal control over financial reporting."[24] The Chamber goes on to state:

> …while Section 404 and AS2 suggest that judgment is called for in assessing terms such as "reasonable" and "material," this judgment has not been applied in the assessment process… Auditing firms have interpreted standards very conservatively requiring excessive documentation and testing of a large number of controls, even those with low risk of preventing or detecting a material error. They felt the need to insist on extensive documentation and testing even where there is a long history of consistently accurate and reliable financial reporting and highly effective management systems. (See page 5)

The Chamber's rhetoric and dissatisfaction with the current internal control assessment regimen continues with the release of another report in January 2006. In this report the Chamber demands that the PCAOB clarify AS2, which is relied upon by management as well as the auditors to implement Section 404. More specifically, this report concludes:

> Auditing Standard #2, the primary implementing standard for Section 404 of Sarbanes-Oxley…doesn't provide much guidance as to when "enough is enough" with respect to auditing of internal controls. Senior PCAOB officials have stated that they can't identify over-auditing. If the primary regulator doesn't know the outer limits of the standards, then how can audit firms or their clients be expected to? The PCAOB's own inspection process—without a standard for determining excessive auditing—encourages auditors, given their structure and liability risks, to continually exceed whatever anyone may think is the standard for control testing and review.[25]

23 See speech by Alan Greenspan at the Asian Financial Centers Conference in Seoul as quoted in "Greenspan Predicts U.S. Governance Revamp." *Financial Times*, April 13, 2006, p. 1.

24 Gupta, Parveen P. and Tim Leech. "Making Sarbanes-Oxley 404 Work: Reducing Cost, Increasing Effectiveness." *International Journal of Disclosure and Governance*, vol. 3, no. 1. April 2006, pp. 1-22.

25 "Auditing: A Profession at Risk." Washington, D.C.: U.S. Chamber of Commerce, January 2006, pp. 14-15.

While the above groups have been overtly criticizing SOX on behalf of their member base, the Financial Executives International (FEI), a trade association representing more than 15,000 cross-listed financial professionals, has conducted periodic surveys[26] of its membership aimed at gauging the cost/benefits associated with implementing Section 404. For example, the fourth survey that was completed just a week after the March 15, 2005, filing deadline for most companies, reported that companies with an average revenue base of $5 billion spent on average "$1.34 million for internal costs, $1.72 million for external costs and $1.30 million for auditor fees.[27] The auditor fees are in addition to companies' financial statement audit fees, on average 57 percent higher."[28] Similarly, the NASDAQ has also been conducting surveys[29] of its issuers, with the most recent one being released in September 2005. Despite the May 15, 2005, guidance issued by the SEC and the PCAOB calling for top-down, risk-based audits, this survey finds that "…the perception of SOX [benefits] is continuing to decline"[30] with only 7% of the respondents reporting that the benefits from Section 404 implementation have improved in year two while 26% reporting worsening of the benefits, and 67% reporting no change in their level of benefits. The following comments made by the NASDAQ survey respondents confirm the fact that lack of and inconsistent application of the current control assessment guidance by the external auditing community is a major source of frustration for most of the registrants:

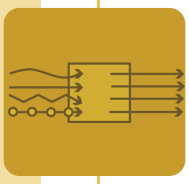
- While SOX itself was relatively clear in concept, the application of the requirements by PCAOB were very delinquent leading to huge confusion and uncertainty.
- Auditors are not applying rules consistently. Audit firms are compelled to be overly conservative and generate higher fees as a result.
- Auditors keep charging more fees. The audit committee cannot say no. Management can't say no. Whoever says no will risk being sued if anything goes wrong…[31]

II.3. The Opening

These pressures, slowly but steadily, have resulted in numerous SEC commissioners increasingly questioning in their public speeches whether the control assessment methodology and the approach suggested by AS2 and/or the external auditing community are at the root cause of the excessive implementation costs. For example, in a speech Paul S. Atkins, one of the SEC commissioners, acknowledges and subtly links the voluminous AS2 to the excessive compliance cost/burden on the SEC registrants:

> As we enter the second year of the 404 process, however, it is becoming increasingly evident that everyone greatly underestimated the costs. When the SEC first released its implementation rules for 404 we estimated aggregate costs of about $1.24 billion or $94,000 per public company. In the SEC's defense, we made this estimate before the Public Company Accounting Oversight Board, or PCAOB, released its 300 page Auditing Standard No. 2.[32]

26 The FEI has conducted a total of five surveys on this topic: May 2003, January 2004, July 2004, March 2005, and April 2006.
27 In the most recent survey of April 2006, FEI reports that average compliance costs are down about 16% during the year-two implementation of SOX 404.
28 "Sarbanes-Oxley: Section 404 Implementation Survey." Florham Park, N.J.: Financial Executive International. March 2005. The survey is available at www.fei.org.
29 NASDAQ Issuer Survey: Sarbanes-Oxley Act, March 2, 2005.
30 NASDAQ Issuer Survey: Sarbanes-Oxley Act of 2002, September 29, 2005.
31 NASDAQ Issuer Survey: Sarbanes-Oxley Act, March 2, 2005.
32 Atkins, Paul A. "Speech by SEC Commissioner: Remarks before the National Association of State Treasurers," September 20, 2005.



Cynthia A. Glassman, also an SEC commissioner, appears more receptive to changes in AS2 in spite of the May 16, 2005, guidance from the SEC and the PCAOB:

> In April of last year, a roundtable…made abundantly clear that the implementation of Section 404 had inappropriately shifted the focus from a top-down, risk-based management perspective to a bottom-up, "check the box" auditor perspective. After the roundtable, the Commission and the PCAOB issued new guidance reminding management and auditors to use seasoned judgment and a risk-based approach in the process. Nevertheless, I continue to hear more about potential misfocus of the Section 404 process and the associated costs…I remain receptive to recommendations to improve the 404 process, including possible changes to AS2.[33]

Commissioner Roel C. Campos acknowledged the cost/benefit imbalance in a recent speech to the International Organization of Securities Commissions (IOSCO) Standing Committee No. 1:

> However, I have to confess that Section 404 is one of the most difficult regulatory issues that I have dealt with in my role as a Commissioner of the SEC. To me, Section 404 represents a classic policy conundrum: What should a regulatory agency do when confronted with a law that has had tremendous benefits, but also has resulted in significant costs?[34]

In the same speech, referring to the recent decision by Canadian Securities Regulators not to adopt the auditor attestation provision of Section 404 and last year's rejection of these requirements by the Turnbull Review Committee of the United Kingdom, Commissioner Campos predicted, "I do not expect convergence on this particular issue."

The lack of follow-up by other jurisdictions with which U.S. capital markets compete for listings and business is becoming a serious cause of concern for the SEC and the U.S. Congress. A recent report, released by the Greater Boston Chamber of Commerce, states:

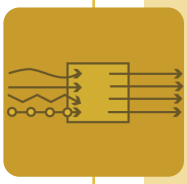
> The number of IPOs in the United States plunged nearly 40 percent in 2005, according to recent figures released by the National Venture Capital Association (NVCA). The organization attributed the lackluster results to a mix of factors, including the uneven technology recovery and higher costs of being a public company imposed by SOX….In 2005, the London Stock Exchange surveyed 80 international companies that conducted IPOs in its markets. The survey revealed that, of those companies that had considered listing on a U.S. exchange, 90 percent felt the demands of SOX made listing in London more attractive.[35]

The steady escalation in the registrants' outcry over costs led to then-SEC Chairman William H. Donaldson announcing in December 2004 "the establishment of an advisory committee to assist the Commission in examining the impact of the Sarbanes-Oxley Act and other aspects of the federal securities laws on smaller compa-

33 Glassman, Cynthia A. "Speech by SEC Commissioner: Remarks before the Tenth Annual Corporate Counsel Institute Priorities and Concerns at the SEC," March 9, 2006.

34 Campos, Roel C. "Speech by SEC Commissioner: Remarks before the Meeting of the International Organization of Securities Commissions Standing Committee No. 1," March 30, 2006.

35 "A Fairer Climb: Improving Sarbanes-Oxley." Boston: Greater Boston Chamber of Commerce, 2006, pp. 12-13.



nies."[36] Applauding the decision to appoint the Advisory Committee on Smaller Public Companies, Alan Beller, then director of the SEC's division of Corporation Finance, stated, "Ensuring that the benefits of securities regulation of smaller public companies outweigh the costs is important to the health of our economy and the role that these companies play in job creation and full employment."[37] Simultaneously, the SEC also tasked COSO to develop an internal control framework to address at least some of the concerns of the small- and medium-sized companies. In response, on October 26, 2005, the COSO Board released for public comment the Exposure Draft of its Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting.[38] Almost after nine months of deliberation, public exposure, and feedback, the COSO Board released the much-awaited final guidance for smaller public companies in a three-volume set on July 11, 2006.[39] According to the Executive Summary accompanying the new guidance, "This document neither replaces nor modifies the Framework, but rather provides guidance on how to apply it. It is directed at smaller public companies—although also usable by large ones—in using the Framework in designing and implementing cost-effective internal control over financial reporting."[40]

II.4. The Call to Action

After going through a deliberative process for more than a year, the SEC Advisory Committee released the much-awaited exposure draft of its Final Report in February 2006 for public discussion and comment. The deadline for submitting comments to the exposure draft was April 3, 2006. In addition to a number of other recommendations, the committee has proposed that the SEC exempt about 78.5% of smaller public companies listed on U.S. stock exchanges from management assessment or auditor certification or both of the Section 404 requirements.[41] This far-reaching proposal has drawn heavy criticism from recent past SEC Chairs: William Donaldson, Harvey Pitt, Arthur Levitt, and Richard Breeden.[42] Additionally, a number of heavyweights[43] from the financial world have collectively written a letter to the current SEC Chairman Cox opposing any such exemption to companies of any size.

36 Press Release 2004-174, "SEC Establishes Advisory Committee to Examine Impact of Sarbanes-Oxley Act on Smaller Public Companies," Washington, D.C.: December 16, 2004.

37 *Ibid*.

38 American Accounting Association. "COSO Releases Small Business Guidance Exposure Draft." Washington, D.C.: October 26, 2005.

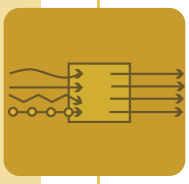
39 "Internal Control over Financial Reporting—Guidance for Smaller Public Companies." Committee of the Sponsoring Organizations of the Treadway Commission: www.COSO.org, July 2006. The format of this guidance is similar to the original COSO 1992 Framework, as Volume 1 contains the Executive Summary, Volume 2 provides the actual guidance, and Volume 3 suggests sample evaluation tools. It is important to point out that with the issuance of the small business guidance we now have three separately titled documents from the COSO Board as follows: (1) the original COSO 1992 Framework along with the related Evaluation Tools, (2) the *Enterprise Risk Management—Integrated Framework* issued in 2004 along with the related Application Techniques, and (3) the *Internal Control over Financial Reporting—Guidance for Smaller Public Companies* along with the related Evaluation Tools.

40 *Internal Control over Financial Reporting—Guidance for Smaller Public Companies*. Committee of the Sponsoring Organizations of the Treadway Commission: www.COSO.org. July 2006, p. 1.

41 For more detailed discussion of the specific exemption criteria, see "Exposure Draft of Final Report of Advisory Committee on Smaller Public Companies" issued by the SEC Advisory Committee on Smaller Public Companies, Washington, D.C.: March 2006.

42 "Former SEC Chairmen against SOX Exemptions." WebCPA, February 24, 2006.

43 They include former Chairman and Chief Executive of TIAA-CREF, John Biggs; former chairman of the Vanguard Group, John Bogle; former Comptroller General of the United States General Accounting Office, Charles Bowsher; former SEC Chairman Arthur Levitt; and former Federal Reserve Chair, Paul Volker.



The following direct quotes from the exposure draft provide insight into the Advisory Committee's thinking behind seeking the exemptive relief for smaller public companies as it pertains to the subject of this research study, which is intended to explore root causes of Section 404 implementation mishaps for companies of all sizes [emphasis added]:

- During the early stages of implementation of Section 404, it became clear that *smaller public companies*, due to their size and structure, *were experiencing significant challenges*, both *in implementing that provision's requirements and in applying the SEC and PCAOB-endorsed COSO Framework*. Many expressed serious concerns about the ability to apply Section 404 to smaller public companies in a cost-effective manner, and also about the *need for additional guidance for smaller businesses in applying the COSO Framework.* [See pages 23-24 under Background of Section 404]
- *COSO* in October 2005 *issued for public comment an exposure draft* titled "Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting." While *intended to provide much needed clarity,* the *guidance has to date received mixed reviews, with many questioning whether it will significantly change the disproportionate costs and other burdens or the cost/benefit equation* associated with Section 404 compliance for smaller public companies. [See page 24 under Background of Section 404]
- First, although AS2 was developed as a guide for *external auditors* in determining whether internal control over financial reporting is effective, *no similar guide has been developed for management*. SEC rules require management to base its assessment of internal control over financial reporting on a suitable, recognized control framework. Although the *COSO Framework* provides criteria against which to assess internal control, it *does not provide management with guidance on how to document and test internal control or how to evaluate deficiencies identified.* Consequently, *AS2 has become the de facto guide for management, even though it was only intended to be used as an auditing standard;* management has tried to meet the same requirements as auditors in performing their assessments, when in fact *management and auditors likely perform their assessments of internal controls differently.* [See pages 27-28 under Origin of Current Problem]
- COSO is developing guidance intended to facilitate the application of the COSO Framework in the small business environment; however, the *draft guidance recently exposed for public comment by COSO does not fully offer a solution for small businesses and may not reduce costs of implementing Section 404* in a small business environment. [See page 28 under Origin of Current Problem]
- Moreover, even though auditors maintain that they are already taking a risk-based approach to the AS2 audit…*implementation of AS2 has resulted in very rigid, prescriptive audits…* auditors applied a *one-size-fits-all standard… auditors* in many instances *utilized an approach that is "bottom-up" rather than "top-down"*…The result is *extensive focus by auditors on detailed processes, a number of which create little or no risk to the integrity of the financial statements.* [In the footnote 74 to this comment, the Task Force noted, "Despite the *May 2005 guidance's* call for a more top-down, risk-based approach, testimony we heard indicated that such guidance *has not substantially altered the approach of auditors.*] [See pages 28-29 under Origin of Current Problem]
- The Task Force Report unequivocally acknowledges the inadequacy of the COSO 1992

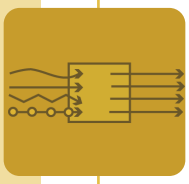
framework when it says "…*Unless and until a framework for assessing internal control over financial reporting for such companies is developed* that recognizes their characteristics and needs…." [See page 40 under Recommendation III.P.1 and page 44 under Recommendation III.P.2]

- Provide, and request that *COSO* and the *PCAOB provide, additional guidance* to help facilitate the assessment and design of internal controls and make processes related to internal controls more cost-effective…Based on the *input provided by COSO* on its framework, *we have concluded that clear guidance does not yet exist* for smaller public company managers on *how to support proper Section 404 assessment of internal controls absent AS2*. While COSO has proposed additional guidance…*we do not think that COSO's revised guidance for smaller companies will result in a cost-effective or proportional alternative for implementing Section 404*. The PCAOB in its January 17, 2006, letter to COSO recommended that *COSO reconsider whether* there is additional, *more practical guidance* that COSO could provide to smaller public companies. [See pages 48 and 50 under Recommendation III.S.1]
- *Determine the necessary structure for COSO* to strengthen it in light of its role in the standard-setting process in internal control reporting. *COSO has been placed in an elevated role* by virtue of being referenced in AS2 and the Commission's release adopting the Section 404 rules….COSO is by far the most widely used internal control framework for such purposes. [See page 52 under Recommendation III.S.2]

The following quotes from selected comment letters submitted to the COSO board on its "Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting" illustrate that the Small Business Advisory Committee is not alone in its grim assessment of the difficulties and challenges the marketplace is facing in conducting its internal control evaluation in accordance with the COSO 1992 Framework to satisfy the Section 404 requirements as implemented by the Final Rule on Section 404 and AS2[44]:

- As for the exposure draft itself, the Board encourages COSO to focus its guidance on the needs of the corporate managements that will implement it, without regard to whether their company's internal control or management's assessment will separately be subject to auditor review or reliance. Even with respect to companies that are subject to requirements that their auditors attest to management's establishment and assessment of internal control, the draft should focus on management's establishment and assessment of internal control over financial reporting. Although management's system and assessment must still be auditable, auditability should not be the primary goal of the guidance. Some of the approaches and examples in the draft may be inappropriate or impractical for the smallest public companies. We recommend that COSO reconsider whether there is additional, more practical advice that COSO could give to such companies. [See PCAOB letter, January 18, 2006, pages 2-3]
- We wish to note, however, that COSO put an artificial constraint on its ability to issue cost-effective guidance geared toward management's needs, by choosing expressly to focus the guidance on evidencing internal control to meet the auditor's perceived needs and

44 All these comment letters are available at: www.ic.coso.org/coso/cosospc.nsf/COSO%20Public%20Comments%20Document.pdf.

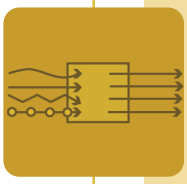


beliefs regarding documentation and testing to comply with AS2. We believe COSO would have been better able to provide guidance that would be most cost-effective for management, if COSO would have started with a blank page and addressed the project from the point of view of what management would need to design, implement, test and attest to the effectiveness of its internal control over financial reporting. Similarly, small public companies that may be exempted from the auditor requirements under Section 404 will still need to file a management report, and they will need to refer to guidance such as COSO's. However, they may not need to meet the standards of AS2, and a COSO built to match AS2 may be excessive for them as being too auditor driven, and not sufficiently management driven, which limits the cost effectiveness of the ED. [See Financial Executives International letter, December 22, 2005, pages 3-4]

- We do have concerns regarding the ability of some very small public companies (e.g., many of those micro-cap companies in the bottom 1 percent of market capitalization) to apply the recommended principles effectively. [See Information Systems Audit and Control Association's letter, January 13, 2005, page 2]
- The IMA is unclear as to how this guidance, built on the existing COSO Framework, tangibly reduces SOX compliance costs for small businesses or businesses of any size. [See Institute of Management Accountants letter, October 24, 2005, pages 1-2]
- While the document will help smaller companies, we do not believe that it will result in substantial reduction in the cost of evaluating and documenting the internal control process by management and the cost to audit internal controls by companies' auditing firms. [See letter from Crowe, Chizek and Company LLC, December 29, 2005]
- Although we believe the Guidance will be an excellent implementation aid, we are less convinced that it will significantly reduce the cost of 404 implementation for smaller companies, at least to the degree expected by some. [See letter by Ernst & Young LLP, January 15, 2006, page 4]
- It is not clear to us, however, that following the prescribed guidance will necessarily help smaller companies "design and implement effective internal control in a cost-effective manner" or lead to cost savings. [See letter from Protiviti Consulting, December 22, 2005, page 1]
- We believe that the COSO guidance should emphasize the use of professional judgment and a risk-based approach that considers the company's individual circumstances when using the 26 principles and related attributes, rather than characterizing each of them as required and expected. [See United States Government Accountability Office letter dated January 20, 2006, page 2]

Although these observations have been generated in the context of smaller public companies, many apply equally to the large companies as well with the only real difference being in their ability to absorb these costs against a larger revenue base. For example, George Honig, audit manager and SOX-compliance head at Sears Holdings, believes that "there is need for a management-centric framework, not just guidance for management. That sort of framework might develop organically over time."[45]

45 Shaw, Helen. "The Trouble with COSO." *CFO Magazine*. March 2006, p. 77.

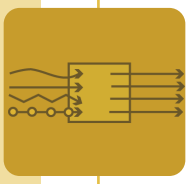


II.5. The Current Situation

Overall, the above discussion and analysis indicates that the current control assessment guidance (AS2 and the COSO 1992 Framework) and the current interpretation of these guides by the external auditors are producing the following undesirable results:

1. High year-one costs with the expectation of lower, but still very significant, year two and ongoing compliance costs. Many registrants and advocacy groups continue to claim that the benefits do not justify the high costs.
2. High external audit costs and widespread ambiguity and disagreement on what constitutes a significant control deficiency and material control weaknesses in accounting disclosure systems.
3. High levels of frustration, dissatisfaction, and confusion with the how-to guidance that has evolved over the past three years.
4. Unequivocal evidence that round-one interpretations of PCAOB guidance resulted in many companies adopting a bottom-up assessment approach. This, in turn, has resulted in repeated admonishments and calls from both the SEC and PCAOB for more risk-based control assessment approaches while complying with Section 404 requirements.
5. Calls from smaller companies for exemption from Section 404 requirements on the basis that current control assessment approaches are too onerous and costly. The SEC's Advisory Committee on Smaller Public Companies has responded by calling for exemption for more than 75% of the SEC registrants from SOX 404 requirements. History suggests that, if exempted, many smaller companies will not put much effort into formally documenting, assessing, and testing their internal control systems when such efforts will not be independently assessed and reported on. This, in turn, could adversely impact their ability to raise capital in U.S. capital markets at favorable cost.
6. The Exposure Draft of the Final Report of Advisory Committee on Smaller Public Companies indicates that the COSO 1992 Framework and AS2 may be contributing to the registrants' and auditing community's failure to implement the true intent of Section 404 in a top-down, risk-based, and cost-effective way.
7. PCAOB's Auditing Standard No. 2 also becoming a "de facto" standard for management guidance.[46]
8. Larger companies, particularly banks that must comply with Basel II requirements, are having difficulty using a process/control-centric approach with broader and more sophisticated operational risk management requirements. Although only a small number of U.S. banks (i.e., maybe 20 or so) are expected to conform to the most onerous Advanced Measurement Approach requirements for operational risk, credit rating agencies and the capital markets in general will expect all financial service institutions to adopt some form of ERM over the next decade.
9. Companies are struggling to integrate Enterprise Risk Management with SOX internal control assessment certifications. The bottom-up/control-centric approach to internal control certifications has led to check-list- and compliance-type mentality in lieu of focusing on real risks facing the business.

46 Consistent with its announcement of May 17, 2006, the SEC issued on July 11, 2006, for public comment a Concept Release Concerning Management's Reports on Internal Control over Financial Reporting. See Release No. 34-54122. This suggests that in the future there may be specific guidance available to the registrants for evaluating and reporting on their internal control effectiveness.



10. Convergence on internal control certification is not on the horizon. For example, many sophisticated capital markets around the world (e.g., Canada, U.K., Australia, and EU) have rejected the validity and usefulness of the SOX 404 assessment and reporting requirements. This, in turn, is impacting the competitive status of U.S. securities markets.[47]
11. Serious concerns continue to exist that current process/control-centric SOX assessment methods in use that entail massive amounts of laborious control documentation and testing will not prevent future Enrons and WorldComs because of a lack of focus and emphasis on the most statistically predictable risks that are known to cause fraudulent and negligent corporate financial reporting.
12. The current focus on extensive, repetitive testing and evaluation of low-level controls will make it very difficult for the accounting profession and registrants to attract and retain high-caliber internal and external audit resources.

In its efforts to make the internal control certifications more relevant and cost-effective, the SEC convened a second Roundtable on May 10, 2006, to seek feedback on year-two Section 404 implementation experiences. Based on the feedback received during this day-long roundtable, the SEC, on May 17, 2006, announced a series of proposed actions that the Commission plans on taking during the remainder of 2006. Among others, these actions include (1) providing guidance for management on how to complete its assessment of internal control over financial reporting, (2) revisions to Auditing Standard No. 2, (3) SEC oversight of PCAOB inspection program, and (4) extension of compliance deadlines for nonaccelerated filers.[48]

III. RESEARCH METHODOLOGY AND SURVEY DEVELOPMENT

This section discusses the research methodology used in designing the survey instrument to collect data for this research.[49] It also describes the sample-selection procedures and presents the respondent and company demographic data to better understand the characteristics of the respondent pool.

According to A.N. Oppenheim, "Questionnaires do not emerge fully fledged; they have to be created or adapted, fashioned and developed to maturity after many abortive test flights."[50] This is particularly true of exploratory studies of the current nature. For an exploratory study, the survey objectives can come from various sources, such as a clearly defined need, review of the literature, and based on the experiences of the knowledgeable experts in a field.[51] Thus, in an exploratory study the researcher starts with ground zero and formulates a number of key

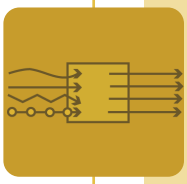
47 See, for example, the United Kingdom deciding against the Section 404-like certifications in "Review of the Turnbull Guidance on Internal Control: Proposals for Updating the Guidance," issued by the Turnbull Review Group on June 16, 2005, p. 5, item 1.15. Also see the press release dated March 10, 2006, issued by the Canadian Securities Regulators canceling all plans to implement the equivalent of Section 404 requirements in Canada by canceling all plans to implement Multilateral Instrument 52-111.

48 "SEC Announces Next Steps for Sarbanes-Oxley Implementation." SEC Press Release 2006-75, May 17, 2006.

49 Gupta, Parveen P. *Internal Audit Reengineering: Survey, Model and Best Practices*. Altamonte Springs, Fla.: Institute of Internal Auditors Research Foundation, 2002, pp. 205-208.

50 Oppenheim, A.N., *Questionnaire Design, Interviewing and Attitude Measurement.* London: Pinter Publishers, 1992, p. 47.

51 Fink, Arlene. *The Survey Handbook.* London: Sage Publications, 2003, pp. 10-11.



issues to investigate as he proceeds in his exploration. Emphasizing the rigor involved in an exploratory study, Oppenheim states that:

> It might be thought that once the main decision about the design of the proposed research has been taken, the researcher would soon be able to make a start with question writing and data collection. This, however, is very unlikely. If we think of any survey as having to pass through a number of stages—from the initial formulation of basic ideas to the specification of the research design, followed by the fieldwork, then the data processing and statistical analysis and so on to the writing of the final report—then we must allow a substantial period of time for construction, revision, and refinement of the questionnaire.[52]

Accordingly, relevant literature and regulatory guidance in this area was reviewed. A number of individuals from the registrant and auditing (internal as well as external) communities were also interviewed on a one-to-one basis in an open-ended setting to clearly understand the challenges confronted by them in conducting control assessments to comply with Section 404 requirements. This process helped in the formulation of the first draft of the survey instrument.

The next step in the research process was to pilot-test the survey instrument. Even though pre-testing or pilot testing slows down the data-gathering process, according to Festinger and Katz:

> It is essential that every new instrument be pre-tested before full-scale field operation. Such pre-testing has three purposes: (1) to develop the procedures for applying the research instrument so that, for example, the scale or schedule can be used effectively with respect to the time it takes to administer; (2) to test the wordings of the questions so that they are suited to the understanding of the audience, and (3) to ensure, as far as is practical, that the specific questions or observations are really getting at the variable for which a measure is needed.[53]

Therefore, nine individuals served as the pilot respondents for the survey. All of them had considerable accounting and auditing experience in the private sector. Many of them had a number of professional qualifications such as CMA, CPA, CA, CIA, etc., and their professional titles, among others, were ex-chief financial officer, corporate controller, director of internal auditing, SOX implementation specialist, external auditor for small public companies, SOX consultant, and a professor. In addition to instructing the pilot respondents to carefully screen each survey question, the respondents were also instructed to (1) identify any important but missing topics or issues related to the focus of the research study, (2) point out (or edit) the ambiguities in the wordings of the survey questions, and (3) suggest ways to contain the length of the survey. As instructed, the pilot participants reviewed the survey instrument thoroughly with many providing feedback in writing and others choosing to provide feedback through a telephone interview. Based on this collective input, a second version of the survey was developed that was again reviewed by a subset of the original pilot participants. The final survey was approved by the Institute of Management Accountants (IMA), the sponsor of this research study, and the Institute of Internal Auditors (IIA), for administration to a large portion of their membership.

52 Oppenheim, p. 47.

53 Festinger, Leon, and Daniel Katz. *Research Methods in the Behavioral Sciences.* New York: Dryden Press, 1953, p. 83.

The final survey had a total of 49 questions divided into four specific sections. Section I contained 10 questions that collected demographic information such as title of the respondent, years in the current position vs. their total working experience, time spent managing SOX, professional certifications, etc., along with information on their company. Section II of the survey contained 10 questions that probed participants on issues facing them while complying with SOX 302/404. Section III of the survey contained a total of 22 questions that specifically dealt with the application of the COSO 1992 Framework for Section 404 internal control assessments. Finally, Section IV of the survey contained five questions that explored the underlying skill set needed to efficiently and effectively execute the control assessment process.[54]

IV. SAMPLE STATISTICS: RESPONDENT AND COMPANY DEMOGRAPHICS

This section is divided into two subsections that respectively discuss (1) sample size, mailing procedures, and response statistics, and (2) respondent and firm characteristics.

IV.1. Sample Size, Mailing Procedures, and Response Statistics

In consultation with the IMA research advisory board, it was decided to post the survey at the www.surveymonkey.com website, a commercial website that specializes in survey administration in a cost-effective and efficient manner.

Two separate surveys were posted at this website: One was accompanied by a cover letter from the CEO and president of the IMA, Paul Sharman, and the other was accompanied with a cover letter from the president of the IIA, Dave Richards. There were no other differences in the content of the two surveys. Since achieving a very high response is always a challenge in survey research, we hoped that endorsement of the survey by the presidents of these two organizations, in the form of a cover letter, would help us in obtaining a reasonably high response rate. In close consultation and under specific directions of the researcher, both organizations selected a large pool of potential respondents from their membership rosters. The IMA selected potential respondents based on the job code classification system and came up with a list of 17,249 potential members. Similarly, the IIA targeted the chief audit executives at the rank of internal audit director or above and came up with a list of 3,793 potential respondents. Additionally, the survey link was also sent to about 874 potential respondents from the researcher's contact database. Except for the IIA, the e-mail link to the survey (with a brief request to complete the survey) was sent directly to all the potential respondents by the researcher. The IIA handled the dissemination of the link to its membership.

The final respondent pool, after taking out the undelivered e-mails, with the related response rate from each group is presented in Table 1.

Overall, given the exploratory nature of this research study and the length of the survey instrument, the response rate of 10% was considered adequate.

54 During the survey administration, many respondents commented that they found the survey questions helpful to get their SOX compliance teams focused on key issues as their company planned its SOX 302/404 compliance project. Since many respondents requested a copy of the survey, it is reproduced in its entirety at the end of this study.

TABLE 1. SURVEY RESPONSE RATE

Type of Respondent Pool	# of Surveys E-mailed	# of Surveys Undelivered or Declined	# of Surveys Actually Delivered	# of Surveys Returned	Response Rate
IMA Members	17,249	858	16,391	1603	9.78%
IMA Members	3,793	*	3,793	324	8.54%
Researcher's Contact Database	874	92	782	171	21.87%
Total	**21,916**	**950**	**20,966**	**2,098**	**10.01%**

*Not captured by the IIA system

IV.2. Analysis of Respondents and Firm Characteristics

IV.2.A. Overall Sample Demographics

This section provides a brief analysis of all the respondents and their related company characteristics. This subsection focuses on discussing respondent demographics for the initial sample of all the 2,098 respondents. The next section provides the same information on the final sample of all the 374 respondents.

As mentioned in Table 1, the total number of responses received was 2,098, yielding an overall response rate of 10%. Table 2 provides information on the job titles/functions of these 2,098 respondents.

TABLE 2. RESPONDENTS BY JOB TITLE/FUNCTION: TOTAL SAMPLE

Respondent's Professional Title	# of Respondents by Title (N=2,098)	% of the Total Sample
Chief Financial Officer	266	12.7%
Vice President	165	7.9%
Controller	459	21.9%
Assistant Controller	75	3.6%
SOX Implementation In-charge/Specialist	110	5.2%
Accounting Manager or Supervisor	231	11%
External Auditor	38	1.8%
Internal Auditor	317	15.1%
Other	437	20.8%
Total	2,098	100%

Given that focus of this research is to document and understand practices related to the management reporting on internal control, it is important to note that almost 62% of the overall responses were from management-oriented positions or nonauditing types. An analysis of the "other" category reveals that a number of these respondents had roles of consultants, small business owners, cost and tax accountants, or other titles unrelated to the study's persons/positions of interest. About two-thirds of the respondent pool had one or more formal accounting- or auditing-related professional certifications such as CPA, CA, CMA, CIA, and CFA. Similarly, more than 85% of the respondents had overall work experience of more than 10 years or more with about 50% reporting work experience of more than 20 years. When probed further, however, almost 50% of the respondents had an experience level of five years or less in their current position, which is generally consistent with current job mobility rates.

In terms of the percentage of time spent by the respondent pool, a significant majority reported spending 30% or more of their time on SOX 302/404 certification-related activities. Only 7% of the respondents reported spending in excess of 75% of their time on SOX 302/404-related projects. Overall, this demographic profile of our respondent pool suggests that we have a very well-experienced and professional respondent pool with significant involvement in SOX-related activities.

When one attempts to gauge the size of the companies represented in our sample, it is significant to note that about 55% of the respondents are from companies with annual revenues of less than $500 million and about 30% are from the companies with annual revenues in excess of $1 billion. When the sample is segmented according to the asset base, the results are essentially the same. In terms of the number of employees, respondents in our sample are evenly split between companies that have 1,000 or more employees and companies with less than 1,000 employees. Although a number of industries (such as healthcare, media and entertainment, construction, mining, agriculture, insurance, high tech, pharmaceuticals, biotechnology, etc.) are represented in our sample, respondents from manufacturing lead the pack with 26%, followed by financial services with 11%, and wholesale/retail with 8%.

When asked about the *current status* of their company with respect to the SOX 302/404 certification, 32% of the respondents are from companies that have already filed their first Section 404 certification, and all these companies are now working on their year-two certification; 14% of the respondents were from companies still working on their first-year certification; 17% of the respondent organizations' were voluntarily conducting internal control assessments in accordance with the requirements of Sections 302 and 404. The remaining 37% of the respondents had nothing to do with the SOX 302/404-related requirements. This is not surprising because the job-code classification scheme employed by professional organizations is rarely up-to-date and complete, thus increasing the possibility of such unsuitable respondents. Eliminating these respondents (794 in total) brings down our initial sample size to 1,304 respondents.

Since the focus of our research study is to document the implementation practices of the accelerated and nonaccelerated filers (both domestic and foreign) as they relate to the use

TABLE 3. RESPONDENTS BY JOB TITLE/FUNCTION: FINAL SAMPLE

Respondent's Professional Title	# of Respondents by Title (N=374)	% of the Useable Sample
Chief Financial Officer	13	3.5%
Vice President	38	10.2%
Controller	43	11.5%
Assistant Controller	16	4.3%
SOX Implementation In-charge/Specialist	66	17.6%
Accounting Manager or Supervisor	20	5.3%
External Auditor	0	0.0%
Internal Auditor	147	39.3%
Other	31	8.3%
Total	374	100%

of the COSO 1992 Framework and other SOX-related issues, we needed to filter out the respondents who were from organizations *other than* an accelerated filer, a nonaccelerated filer, or a foreign filer, and those that did not use COSO 1992 as the control framework to conduct their internal control evaluations. This filtration further brought down our sample size considerably. The final sample size consists of 374 respondents—approximately 18% of the 2,098 respondents who responded to the survey. While our filtration and screening process brought the number of final useable responses to 374 from 2,098 total respondents, this level of screening ensures a more robust and targeted sample from which to draw inferences.[55] Thus, we present below the demographic profile of only the 374 respondents to provide an appropriate context for interpreting the findings of this research study as discussed in the next section.[56]

IV.2.B. Final Sample Demographics

Table 3 provides information on the current job titles and functions of the final sample of 374 respondents. A review of this table suggests that about 39% of the respondents are from internal auditing and 53% of the respondents work in a wide variety of finance- and accounting-related positions. The remaining 8% are in the "Other" category, which includes respondents with titles such as internal consultant, financial analyst, compliance director, SOX steering committee member, audit committee chair, president and CEO, risk manager, etc. It is

55 It is not uncommon in studies of such a nature for the final useable sample to be significantly lower than the initial response rate. Further, our response rate compares favorably to other SOX surveys conducted by other researchers as mentioned in Section I.

56 It should be noted that from here on all data analysis is based on the responses of these 374 survey participants.

TABLE 4. PERCENTAGE OF TIME SPENT ON SOX 302/404 COMPLIANCE

% of Time Spent	# of Respondents by Title (N=374)	% of the Useable Sample
<= 10%	46	12.3%
11%–20%	72	19.3%
21%–30%	59	15.8%
31%–40%	36	9.6%
41%–50%	31	8.3%
51%–75%	45	12.0%
> 75%	85	22.7%
Total	374	100%

important to note that there are no external auditors represented in our survey since we were only interested in the company-specific experiences.

Further analysis of the demographic data indicates that about 75% of the 374 respondents have one or more of the following formal auditing and accounting certifications: CPA, CMA, CA, CISA, and CIA. More than 70% of the respondents have an overall work experience of more than 15 years, with 60% being in the current position anywhere from one to five years. Besides having significant finance and accounting experience, respondents in our sample also spend considerable time on the SOX 302/404-related matters. Table 4 presents data in answer to the following question:

- What percentage of your time is spent managing or working on the projects related to SOX 302/404 compliance?

The data presented in Table 4 can be used to group respondents into three distinct clusters: the first one-third of the respondents spend less than 20% of their time working on 302/404 compliance projects; the middle one-third spend about 21% to 50% of their time on SOX 302/404 compliance projects; and the final one-third spend more than 50% of their time on SOX 302/404 compliance projects.

Overall, given the experience level of survey respondents combined with the amount of time they spend on managing SOX 302/404 compliance projects, we believe we have a very seasoned pool of survey respondents. Consequently, the findings and discussions presented in the next section should be of importance to various policy makers including the standard setters and the regulatory bodies as they strive to enforce these new rules as well as provide guidance to implement the Section 302/404 requirements in a cost-effective manner.

In addition to having a very well experienced respondent pool, the external validity of our research findings extends to companies of all sizes because our sample includes respondents from companies of varying sizes in terms

TABLE 5. RESPONDENT FIRM SIZE BY REVENUE AND ASSETS

Company Size	Interval	Total Revenue (N=374)		Total Assets (N=374)	
		# of Respondents	%	# of Respondents	%
Small	<= $100 million	41	11%	34	9%
	> $100 million <= $500 million	64	17%	54	14%
	Small-Size Companies	**105**	**28%**	**88**	**23%**
Medium	> $500 million <= $1 billion	51	13%	50	13%
	> $1 billion <= $5 billion	88	24%	83	22%
	Medium-Size Companies	**139**	**37%**	**133**	**35%**
Large	> $5 billion <= $10 billion	41	11%	36	10%
	> $10 billion	81	22%	96	26%
	Large-Size Companies	**122**	**33%**	**132**	**36%**
	Not Disclosed	8	2%	21	6%
	Total	374	100%	374	100%

Note: Percentages are rounded.

of revenue and asset base. Table 5 presents this information. When we cluster our sample of 374 respondents in three major categories of small (less than 500 million), medium ($500 million to $5 billion), and large (more than $5 billion) companies, based on total revenue and assets, we find that our sample is reasonably evenly distributed with a slight bias toward fewer respondents from smaller public companies.

Table 6 presents information on the respondents represented in our sample based on company size as measured by the number of employees. About 19% of the respondents represented in our sample are from companies with 1,000 or fewer employees. The remaining 81% of the respondents are somewhat evenly divided into two broader groups of companies having employees anywhere from 1,001 to 7,500 and more than 7,500. Dissecting our sample by number of employees again confirms that we have fewer respondents in our sampling frame from smaller public companies.

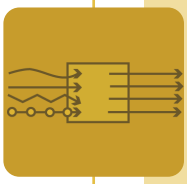
To round out the discussion of the demographic characteristics of our sample, Table 7 lists the major industries represented in our final sam-

TABLE 6. RESPONDENT FIRM SIZE BY NUMBER OF EMPLOYEES

Company Size	# of Employees	# of Respondents (N=374)	% of Respondents
Small	<= 500	39	10.4%
	501–1,000	31	8.3%
Medium	1,001–2,500	62	16.6%
	2,501–5,000	64	17.1%
	5,001–7,500	27	7.2%
Large	7,501–10,000	16	4.3%
	10,001–15,000	24	6.4%
	> 15,000	111	29.7%
	Total	**374**	**100%**

TABLE 7. INDUSTRY COMPOSITION OF THE RESPONDENT POOL

Industry	# of Respondents (N=374)	% of the Total Sample
Manufacturing	105	28.0%
Financial Services	53	14.2%
Transportation, Communication, and Utilities	42	11.2%
Wholesale/Retail	34	9.0%
Business Services	26	7.0%
High Tech	18	4.8%
Insurance	16	4.3%
Healthcare	13	3.5%
Construction, Mining, Agriculture	13	3.5%
Pharmaceuticals and Biotechnology	11	2.9%
Media and Entertainment	10	2.7%
Energy, Oil, and Gas	8	2.1%
Real Estate	6	1.6%
Aerospace and Defense	4	1.1%
Miscellaneous	15	4.1%
Total	**374**	**100%**



ple. The industry classification scheme is the same one that IMA used in collecting data from its membership at the time of the study. Although there are a number of industries represented in the sample, almost 60% of the respondents in our final sample come from the following four industries: manufacturing; financial services; transportation, communication, and utilities; and wholesale/retail.

With regard to the SOX 302/404 filing status of the respondents, 73% of the 374 are from accelerated filer companies, 21% are from nonaccelerated filer firms, and about 6% represent foreign filers. Similarly, 75% of respondents are from companies that have already filed their first SOX 302/404 certification, and the remaining 25% are from companies currently working on filing their first certification.

V. SURVEY RESULTS AND DISCUSSION OF FINDINGS

This section is subdivided into two sections. Subsection 1 informs the reader about various screens used to analyze the survey results in subgroups and how to interpret survey findings. Subsection 2 presents the key results and the discussion of survey findings. In this subsection, wherever appropriate, analysis of the survey results is supplemented with the discussion of written comments by the survey participants. Relevant regulations and standards are also discussed along the way to interpret the results and highlight the implications of the current implementation practices.

V.1. Brief Note on Interpreting the Survey Results

The survey results are presented in various tables throughout this research study. When interpreting the results, the reader should keep in mind that all respondents may not have answered every single question in the survey. Thus, to eliminate the problem of uneven responses, we have presented all results in percentages. However, information on the absolute number of respondents is also provided next to each percentage along with the overall or base sample size for each table. The base for each question is the number of respondents answering that particular question. Sometimes, the percentages may not add up to 100%. This is either due to a respondent being allowed to pick more than one choice in the question or rounding errors in computing percentages.

Since our survey participants include respondents currently working in the accounting and auditing positions, wherever appropriate, to provide a richer discussion, we have segmented our sample into two subgroups: internal auditors and management-types. The following position descriptions are included in the management-types: chief financial officer, vice president, controller, assistant controller, SOX implementation in-charge/specialist, accounting manager or supervisor, etc. Similarly, a subgroup based on number of employees was also created for analysis purposes to understand if there are any systematic differences in companies of varying sizes. It is important to note that whenever we conduct subgroup analysis, it is conceivable that our results in that case are based on a smaller sample size. From a research methodology viewpoint, caution should be used in drawing conclusions from such results. Also, the percentages computed for our subgroup analysis are based on the total number of respondents in that particular subgroup.

V.2. Key Results and Discussion of Findings

This section is organized into four subsections that cover issues related to (1) SOX 302/404; (2) risk-based assessment approach; (3) using

COSO 1992 as the control evaluation framework; and (4) components of the risk and control assessment skill set. Each of these subsections may have several subareas under them. While discussing the findings in each one of the subareas, we first present and discuss results and findings for the entire sample of 374 respondents. We then segment this sample using two different filters. First, we cluster the survey respondents into two distinct categories along their job titles: management-types vs. internal auditors. The reason for this filter is to understand whether there are any significant differences in the opinions of these two groups of respondents because *a priori* one would expect the opinion of auditors to differ from those of management-types because traditionally auditors are more control-centric in their thinking and approach while management is more risk-focused. Second, we divide the sample by company size (small vs. medium to large) to discern whether implementation practices significantly differ between the small-firm respondents and the medium to large firm respondents while complying with the SOX 302/404 requirements.

There is considerable debate in the governance literature about what creates complexity and the potential for breakdown in a company's system of internal control over financial reporting. The general criteria that have typically been used to measure complexity involve one or more combinations of the following metrics: total revenues, total assets, market capitalization, number of employees, and the number of segments or countries in which a company operates. The recently released *Exposure Draft of Final Report of the SEC Advisory Committee on Smaller Public Companies* uses a combination of market capitalization and revenue to classify firms in the smaller public company definition. Unfortunately, there is no single standard metric that is universally acceptable to define what constitutes a smaller public company with respect to the complexity in its system of internal control over financial reporting. In this study, in the absence of broadly accepted categorization criteria, we have elected to use number of employees to segment our sample into small and large companies. Thus, for the purposes of this research study, we defined a company with 1,000 or fewer employees as a smaller company. Conversely, a company with more than 1,000 employees is considered to be a medium-to-large company. We considered lowering the threshold for a smaller company to 500 employees but, given our sample, that resulted in an extremely lopsided sampling frame (only 39 companies in our sample report 500 or fewer employees), challenging us to draw any meaningful conclusions from that data (See Table 6 for response rate by number of employees).

V.2.A. SOX 302/404-Related Issues

V.2.A.1. Accountabilities for SOX Compliance Work

There has been considerable debate in the SOX community regarding what role and responsibility should be assigned to various functions or departments in the organization to comply with the requirements of Sections 302 and 404. There is no disputing the fact that according to these two sections, management is primarily responsible for producing reliable financial statements and disclosures and ensuring that the internal control system that supports or underlies all financial disclosures is working effectively during the time period covered by the periodic financial disclosures. In practice, however, the word "management" connotes many organizational participants, including process owners, financial reporting personnel responsi-

ble for consolidating and preparing the quarterly and annual financial disclosures, office of the chief financial officer, controller, treasurer, etc., internal auditors, and any other group specifically charged with the responsibility to oversee the financial reporting process.

To better understand the involvement of various groups in the SOX compliance process, we identified eight primary activities and five primary groups, based on pre-survey interviews, that would be potentially involved in SOX 302/404 compliance-related projects. Table 8 presents what our survey respondents report on the roles and responsibilities of various groups in their company as it relates to SOX 302/404 work.

A review of the data presented in Table 8 suggests that, at least during the initial round of SOX compliance, the internal auditors and the process owners appear to be assuming the lead role in helping their company comply with Sections 302/404.

It is important to note from Table 8 that the process owners in the organizations are taking the lead in *creating* (58%) and *maintaining* (60%) *the process documentation* as well as *conducting the self-assessment of the process* (46%) and the related *remediation actions* (72%). The involvement of the process owners in all of these four activities is logical and consistent with the spirit of SOX. As discussed

TABLE 8. RESPONSIBILITIES FOR SOX COMPLIANCE WORK

SOX Compliance Activity	Groups/Functional Units Involved in SOX Compliance Activity (N=372)				
	Entity-level Compliance Group	Internal Auditing	Financial Reporting Function	Operations or Process Owners	IT
1. Creating Process Documentation	19% (70)	45% (166)	34% (125)	58% (216)	30% (112)
2. Maintaining Process Documentation	19% (69)	32% (119)	33% (123)	60% (225)	27% (102)
3. Identification of Risks	31% (117)	63% (234)	37% (137)	37% (139)	21% (77)
4. Identification of Related Controls	28% (103)	59% (221)	38% (143)	45% (168)	26% (97)
5. Testing of Key Controls	15% (55)	77% (285)	20% (76)	24% (88)	15% (56)
6. Self-Assessment	14% (53)	18% (67)	26% (96)	46% (172)	16% (61)
7. Remediation of Exceptions	19% (69)	23% (85)	41% (152)	72% (267)	33% (121)
8. Coordinating with External Auditors	28% (104)	63% (234)	40% (147)	6% (22)	7% (27)

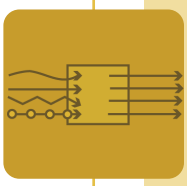
Note: Percentages are rounded. If percentages do not equal 100%, it is because more than one function within a company can be involved in performing a given activity.

below, however, it appears that the internal auditing function is also assuming a dominant role in many companies by actively helping their company management comply with the SOX 302/404 certification requirements.

The activity of identifying risks is critical to the overall validity of the control assessment work and conclusions arrived at. According to Table 8, 63% of the respondents indicated that internal auditors are spearheading this critical aspect of the SOX compliance process. Consistent with the SOX goal of management ownership of identifying related risks, one would expect that a larger number of companies will involve the process owners as well as the financial reporting function in this area. But we find that each one of these two groups were mentioned only 37% of the time for this critical activity. If the process owners in an organization are unable to identify the risks to the financial reporting as impacted by their process, how would they design effective controls to mitigate any such risks? Thus, given that the spirit of the SOX is management accountability for mitigating the risks (or control effectiveness) to unreliable financial reporting and disclosure, it is somewhat puzzling to find internal auditors assuming the dominant role in risk identification (63%) and testing of key controls (77%). There is nothing wrong in theory about the involvement of the internal auditors in the SOX compliance process so long as they are internally auditing the process undertaken by process owners (i.e., management) to identify and mitigate the risks to reliable financial reporting.

From the results presented in Table 8, another puzzling finding is that more internal auditors (63%) than the financial reporting personnel (40%) are involved in coordinating SOX 302/404 certification with their company's external auditors. By this comparison, we do not suggest that internal auditors should not at all be involved in coordinating some aspects of the internal control audit with their company's external auditors. However, it is the dominance of the involvement of internal auditors that causes us to question whether, directly or indirectly, some internal audit departments are assuming the role and at least some of the key responsibilities of company management when it comes to SOX 302/404 compliance. These findings persist even when the responses of the internal auditors are removed from the sample to eliminate any potential self-serving bias that the inclusion of internal auditors may introduce.

Further, the same relationship holds true even when we analyze the response of only the medium to large companies with more than 1,000 employees. However, the situation changes when we examine the responses of the small companies with less than 1,000 employees. The financial reporting function gains more prominence. For example, for creating the *process documentation* activity the financial reporting function (47%) shares in the workload almost equally with the internal auditing function (46%) and the operation or process owners (43%). Similarly, for the *identification of related controls* activity, the internal auditing and the financial reporting function each share equally (49% each) in the work. For *coordination with the external auditors,* the financial reporting function (54%) is more often mentioned than the internal auditing function (47%). Interestingly in medium to large companies more internal auditors (67%) are involved in coordinating their company's audit with the external auditors than the financial reporting function (36%). This finding is



consistent with the fact that more medium to large companies have a separately established internal auditing department than do smaller public companies.

Debating the implications of these findings, we believe that for management to truly own the responsibility for reliable financial reporting processes, the task of identifying risks and testing whether the related key controls are working, ideally, should be in the realm of management only. This should not be construed to mean that internal auditors should not be "at the table" when it comes to SOX 404 compliance. In our opinion, internal auditors can contribute a great deal to the SOX 404 compliance project by attesting to the consistency and quality of the process employed by management to test the effectiveness of the company's system of internal control over financial reporting. As part of this attestation, the internal auditor can provide assurance on some of the following aspects of this process: (1) Does management follow the process on a consistent basis, across the board, and throughout the organization? (2) Is the process rigorous enough to assure that "more than inconsequential" control deficiencies will be detected? (3) Do the individuals testing the operating effectiveness of the controls have sufficient training in conducting an internal control assessment? (4) Do the self assessments conducted by the process owners demonstrate "fidelity" between the documented effectiveness of controls and their actual operating performance and design effectiveness?[57]

However, given the frantic pace of compliance activity during the initial implementation of the Section 404 requirements, from a practical standpoint, it was not entirely unreasonable to expect internal auditors being called upon to take a lead role in executing these activities because they are often the main group that possesses the time and necessary competencies to conduct formal risk and control assessments. Later in this study we will discuss in detail the implications of deficient skill-sets and related competencies in the management to effectively discharge their responsibilities under SOX.

We think it is important to raise a red flag at this point: If this trend does not reverse itself in the future, it will result in questions about the independence and objectivity of the internal auditing function in such companies. Further, if management certification of the effectiveness of the company's internal controls over financial reporting is based entirely on the assessment and testing done by the company's internal auditors and these certifications are later found to be inaccurate or misleading, there is every conceivable potential that the plaintiff's bar may construe this excessive reliance on the work of the internal auditor as equivalent to gross negligence on the part of company management, with commensurate liability implications. Although the notion of "independence" in the case of internal auditors is not at the same level as external auditors, it is nevertheless

57 For example, at one of the major *Fortune* 500 companies there is a clear demarcation of accountability between the responsibilities of the finance and the internal audit function. The finance function is responsible for risk identification, key control selection, design conclusions, remediation, and deficiency assessments, and the internal auditing function is responsible for the operating effectiveness testing. The reason internal auditors have been assigned operating effectiveness testing is largely due to the sheer size and the decentralized nature of operations in this company. According to the SOX Compliance Project team, such an approach not only provides a cost-effective solution to SOX 404 compliance but it also ensures that formal testing, on which the management finally bases its certification, is not only of high quality but is also done consistently throughout the organization by the people trained in testing internal controls.

important to remind the internal auditing community that according to the Institute of Internal Auditors (IIA):

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Thus, according to this definition, internal auditors are to remain independent and objective[58] by auditing the related processes rather than assuming the primary role for any of the eight activities as presented in Table 8. Whether this trend reverses in future years is a matter of critical importance and a relevant subject for further research and study. The IIA, the leading international organization that governs the internal auditing profession, should be on the lookout for any signs indicating whether the independent and objective internal auditing activity is morphing into a management function. Internal auditing is the third leg of the proverbial governance stool (in addition to the board and the external auditors), and any such metamorphosis would not serve the internal auditing profession and the registrant community well. Through its quality control inspection requirements, the IIA can help ensure that internal auditing remains an independent and objective activity. Also, the company's board of directors—including the audit committee—should be cognizant of the legal liability implications and ensure that while complying with Sections 302 and 404, the company management "in fact" owns the internal control assessment process and does not outsource it to the company's internal auditors to the point where it is construed as an abdication of their responsibility under SOX 302/404.

V.2.A.2. Cost of Compliance

As mentioned earlier in Section II, a number of private groups and professional organizations have been regularly conducting surveys of various companies to report on the massive compliance costs imposed by the implementation of Sections 302 and 404 requirements. In the SOX community, analysts generally use a rule of thumb of one million per billion in revenue to indicate what it is costing them to comply with Sections 302 and 404 requirements. However, none of the surveys and studies that we have reviewed focused in great detail on the root causes that are behind the high SOX costs that most expect to continue in the future.

In this subsection, we first focus on which SOX compliance activities are driving the costs being incurred and then explore the extent to which the potential cost drivers are contributing to the excess costs in our respondents' organizations. Table 9 presents the findings on SOX compliance-related activities that were costly to the companies participating in our survey.

Table 9 indicates that (1) creating and maintaining process documentation (34% said somewhat costly and 58% said very costly) and (2) testing of key controls (44% said somewhat costly and 48% said very costly), undoubtedly, were two activities that were considered somewhat to very costly by more than 90% of the survey participants. Attestation and certification was a close third with about 70% (33% said somewhat costly and 36% said very costly), followed closely by the remediation-related activities at 65% (47% said somewhat costly and 18% said very costly). The more balanced mix

58 See the IIA Standard #1100 as published in *The Professional Practice Framework*, January 2004.

TABLE 9. COST OF SOX COMPLIANCE-RELATED ACTIVITIES

	Extent to which SOX Compliance Activities Are Costly (N=372)			
SOX Compliance Activity	Not Costly At All	Not Particulary Costly	Somewhat Costly	Very Costly
1. Creating and Maintaining Process Documentation	0	8% (31)	34% (126)	58% (214)
2. Testing of Key Controls	0	7% (25)	44% (162)	48% (177)
3. Self-assessment by Process Owners	5% (19)	32% (118)	31% (117)	8% (31)
4. Remediation-related Activities	1% (5)	32% (118)	47% (174)	18% (67)
5. Attestation and Certification	2% (9)	22% (81)	33% (124)	36% (134)
6. Staff Training	2% (97)	39% (145)	45% (166)	12% (144)
7. Investment in New Tools and Technology	6% (23)	31% (114)	34% (128)	16% (60)

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

of responses for staff training and investment in new tools and technology could also suggest that in order to cope with SOX, companies have simply not been able to catch their breaths and invest in internal staff training and technology to squeeze more value out of their SOX compliance efforts.

About 25% of the respondents indicated that self-assessment by the process owners was not conducted at their company. Of the 75% of respondents who reported that process owners did conduct a self-assessment in their companies, only 31% considered this to be a somewhat costly activity. These findings are consistent with the literature and the practical experience of numerous organizations, as documented through various Control and Risk Self Assessment (CRSA) conferences organized by the Institute of Internal Auditors. Generally, self-assessed organizations report lower monitoring costs when compared with the organizations relying heavily on direct report auditing, which is driven largely by assurance specialists.

Looking at the last two activities reported in Table 9, it appears that about 50% of respondents believe that staff training and investment in tools and technology to comply with SOX were also somewhat to very costly activities for their organization to bear. These findings do not significantly change when we analyze the sample by firm size.

When asked whether their company is experiencing an increase or decrease in their SOX compliance costs, relative to their initial year implementation costs, an overwhelming large majority of our respondents reported that they experienced a significant decline in their cost of SOX compliance all across the board. These results are summarized in Table 10.

TABLE 10. PERCENTAGE INCREASE OR DECREASE IN SOX COMPLIANCE COSTS

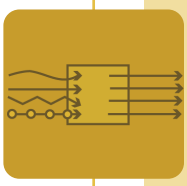
SOX Compliance Activity	% Reporting Decrease	By How Much Relative to Year One? (N=372)		
		0%–10%	11%–20%	> 20%
1. Creating and Maintaining Process Documentation	72% (267)	16% (40)	21% (52)	60% (149)
2. Testing of Key Controls	62% (230)	31% (68)	28% (62)	34% (74)
3. Self-assessment by Process Owners	37% (138)	35% (61)	18% (31)	19% (32)
4. Remediation-Related Activities	69% (255)	38% (93)	22% (52)	33% (80)
5. Attestation and Certification	57% (212)	51% (107)	21% (44)	19% (39)
6. Staff Training	55% (203)	41% (82)	21% (41)	28% (55)
7. Investment in New Tools and Technology	31% (115)	20% (31)	10% (15)	36% (54)

Note: Percentages are rounded. When the totals do not add up to 100% for an activity, either the activity was not applicable to the company or there was no change in its costs.

The results in Table 10 indicate that almost three out of every four respondents believe that their company is experiencing a decline in costs related to creating and maintaining process documentation. This is good news and in line with the expectations. However, what is more encouraging is that 60% of them are reporting a decline of more than 20% in such costs. Although a significant number of respondents reported a decline in costs related to the testing of key controls as well as attestation and certification, the magnitude of decline is much lower for these two activities when compared with the cost reductions experienced by companies for their process documentation-related activities.

These findings support two commonly held beliefs. First, maintaining process documentation is not as expensive as it is to create in the first place. There is no doubt that a number of registrants had a lot of deferred maintenance to do to bring their core internal control over financial reporting (ICoFR) process documentation up-to-date. As a result, the registrants experienced higher costs during the year-one compliance cycle followed by the reduction in such costs during year two. Second, the reason significant cost reductions are not expected for activities related to the testing of key controls and attestation and certification may very well be attributed to the external auditors not using a top-down, risk-based approach as directed by the SEC and PCAOB. On September 20, 2005, while expressing doubts about major cost reductions in year two, SEC Commissioner Atkins[59] conceded that "we are now starting to hear that cost

59 Atkins, Paul S. "Speech by SEC Commissioner: Remarks before the National Association of State Treasurers," September 20, 2005.



reductions for year two of the Section 404 process will not approach the 50% reductions on which many had been counting. Cost reductions from year one will instead be in the neighborhood of 5%–20%, and I predict that the reduction will be at the low end of this range."

Costs are also expected to decline for activities such as (1) self- assessment by process owners, (2) remediation of internal control weaknesses, and (3) staff training, but again not to the same extent as for process documentation. Investment in new tools and technology is the only area where a little more than one-third of our respondents (37%) are expecting the costs to go up. This is also consistent with the prevailing belief that during year two and year three the companies are more likely to think about automating and cost-optimizing the SOX compliance process. We do not see any major differences in the cost of various activities when we segment and analyze the sample by company size (i.e., small vs. large companies). We should note that a reduction in SOX compliance costs over time, while expected to some degree after the initial shock, implies nothing about the value or cost-benefit associated with the SOX compliance activities.

Besides exploring which SOX 302/404 compliance-related activities are costly to the companies participating in our survey, we also sought to understand what factors may be contributing to the increased cost burden experienced by these companies. As discussed in Section II, the massive cost associated with the internal control certifications has become the "talk of the town" and a major call to action from the opponents of these requirements. There is merit to the argument presented by the detractors of SOX that, in a market-based system, unless the cost to comply with regulatory requirements is commensurate with the benefits received, it erodes shareholder value. As sound as this argument is in theory, however, it is based on a presumption that the benefits derived by all stakeholders are objectively measurable and can be quantified in dollar terms. This may not necessarily be the case when it comes to measuring the intangible benefits (e.g., reliable financial reporting and disclosures to capital markets) associated with complying with Section 404.

Consistent with the focus of this research study and based on the feedback received during our pre-survey interviews, we developed the following list of potential factors that may appear to be contributing to high SOX compliance costs:

1. Lack of a generally accepted assessment criteria/framework available while evaluating the effectiveness of our system of internal controls.
2. Difficulty in using the COSO 1992 Framework in arriving at a consensus opinion on the effectiveness of our system of internal controls.
3. External auditors' insistence on documenting and testing all processes irrespective of the residual risk profile of these processes.
4. Lack of practical guidance from the SEC or other professional organizations on how to accomplish the task of deciding what constitutes an effective or ineffective internal control system.
5. Lack of practical guidance from the SEC on what exactly is a significant deficiency vs. material control weakness.
6. Redundant testing performed by external auditors and internal auditors or SOX compliance group due to the inability of these groups to collaborate to reduce the sample size.

TABLE 11. SOX 302/404 POTENTIAL COST DRIVERS

Potential Cost Drivers	Overall Sample (N=372)		Internal Auditors (N=145)		Management Types (N=227)	
	No Extent to Some Extent	Moderate to Large Extent	No Extent to Some Extent	Moderate to Large Extent	No Extent to Some Extent	Moderate to Large Extent
1. Lack of a generally accepted assessment criteria/framework available while evaluating the effectiveness of our system of internal controls.	52% (191)	45% (169)	58% (85)	40% (58)	47% (106)	49% (111)
2. Difficulty in using the COSO 1992 Framework in arriving at a consensus opinion on the effectiveness of our system of internal controls.	73% (269)	24% (86)	82% (118)	16% (24)	66% (151)	28% (62)
3. Our external auditors' insistence on documenting and testing all processes irrespective of the residual risk profile of these processes.	38% (142)	59% (217)	42% (61)	57% (82)	36% (81)	59% (135)
4. Lack of practical guidance from the SEC or other professional organizations on how to accomplish the task of deciding what constitutes an effective or ineffective internal control system.	28% (105)	68% (253)	31% (45)	67% (97)	27% (60)	68% (156)
5. Lack of practical guidance from the SEC on what exactly is a significant deficiency vs. material control weakness.	41% (153)	55% (206)	46% (68)	50% (73)	37% (85)	59% (133)
6. Redundant testing performed by external auditors and internal auditors or the SOX compliance group due to the inability of these groups to collaborate to reduce the sample size.	32% (118)	64% (238)	38% (56)	58% (83)	28% (62)	68% (155)

Note: Percentages are rounded. When the respective totals do not agree either to the overall sample size or sub-sample categories, the difference represents the number of respondents choosing the "Uncertain" response.

Table 11 presents the results for these six potential cost drivers by summarizing the responses for the overall sample as well as for two subcategories. As discussed in the beginning of this section, the two subcategories are created to represent two distinct groups: internal auditors and noninternal auditors, whom we label as management-types. The reason to segment our sample into these two groups is to explore whether each group views the impact of the presented factors (or cost drivers) differently because of their position in the organization. The internal auditing group certainly has more of an assurance-type mindset that may be somewhat biased toward a control-centric approach to internal control evaluation when compared with the management-types, whom we would expect to be more focused on the management of risks to acceptable levels.

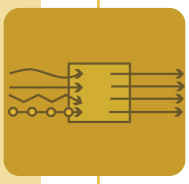
In looking at the overall sample, two factors (#4 and #6) are most often quoted by the survey respondents as having a moderate to large impact on their overall SOX 302/404 compliance costs. Factor #4, "Lack of practical guidance from the SEC or other professional organizations on how to accomplish the task of deciding what constitutes an effective or ineffective internal control system," was cited by 68% of the respondents in our overall sample. When we analyze this result by auditor and management-type, we find significant convergence in the opinion of these two groups on this factor as a significant cost driver.

To better understand why lack of practical guidance in deciding what constitutes an effective system of internal control is topping the list as a major cost driver, we must concurrently examine the results on factor #1, which explores the extent to which the lack of a generally accepted assessment criteria/framework to evaluate the effectiveness of a system of internal control contributes to the excess costs. For the overall sample, about 45% of the respondents believe that this factor also contributes in moderate to large extent to the high compliance costs being incurred. However, when analyzed by subgroups, more management-types (49%) than internal auditors (40%) attribute excess cost to the lack of availability of a generally accepted assessment criteria or framework. This difference in the responses is perhaps due to inherent differences in the orientation and background of these two groups.

Further, since complying with Sections 302 and 404 requires company management and their external auditors to arrive at a binary yes or no conclusion on the effectiveness of their internal control over financial reporting, we question how a company's management and external auditors form their opinions in the absence of a "practical and generally accepted control assessment criteria." At least some argue that the COSO 1992 *Internal Control—Integrated Framework* provides the necessary criteria to form such a binary opinion. Paragraph 14 of the PCAOB Auditing Standard No. 2 (AS2) explicitly endorses COSO 1992 as an acceptable framework by stating that:

> In the United States, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) has published *Internal Control—Integrated Framework*. Known as the COSO report, it provides a suitable and available framework for purposes of management's assessment. For that reason, the performance and reporting directions in this standard are based on the COSO Framework.

There is no doubt that the creation of the COSO 1992 Framework, almost 15 years ago, was a significant milestone and contribution to better



understand the concept of internal control. According to R. Malcolm Schwartz, one of the principal contributors of the Coopers & Lybrand team that wrote the COSO 1992 guidance, "The Framework was developed in response to the Treadway Commission's findings on fraudulent financial reporting to answer two key questions: one, what is internal control? And second, how do I know that I got it?"[60] The intent behind raising these two questions was to unify or reconcile a variety of competing definitions of internal control in existence at that time and to clarify for all what is internal control. Thus, the focus of the Coopers & Lybrand team was to provide broader-level guidance on the concept of internal control. Certainly, the group did not expect that their framework would be used sometime in the future to unequivocally conclude whether a company's internal control over financial reporting is effective or ineffective. In writing the preface of his book, Steven Root states, "The more research and inquiry I performed, the more I became concerned that the COSO Framework may not be the most suitable criteria for senior executives to use in helping to decide on internal control sufficiency."[61]

Given the above comments from the practitioners who are close to the action, we should note that only one out of every four respondents in our sample believes that "difficulty in using the COSO 1992 Framework in arriving at a consensus opinion on the effectiveness of our system of internal controls" (factor #2) is a significant cost contributor. On the surface, these findings may appear to contradict some of the above arguments. However, when asked which of the following two statements is "more true" for first-year SOX certification efforts, 62% of the respondents chose AS2, and this result does not change even when we analyze the responses in our sample by internal auditors and management-types:

1. Majority of our internal control assessment was largely guided by and conducted in accordance with the PCAOB Auditing Standard No. 2.
2. Majority of our internal control assessment was largely guided by and conducted in accordance with the COSO 1992 Internal Control Framework.

Thus, it is the dominance of AS2 in guiding the SOX control assessments that explains why our respondents do not think that "difficulty in using the COSO 1992 Framework in arriving at a consensus opinion on the effectiveness of our system of internal controls" (factor #2) is a major contributor to high costs. Regardless of the real or perceived drivers of high SOX compliance costs, these results suggest that there is sufficient ambiguity about the practical and how-to guidance that company management can use to comply with SOX 404 while concurrently mitigating the real threats to reliable financial reporting.

Examined further, since Paragraph 14 of AS2 states that its "performance and reporting directions are based on the COSO Framework," few survey respondents wondered whether the distinction presented in the above two statements is somewhat artificial. According to the PCAOB, "The directions in Auditing Standard No. 2 are based on the internal control framework established by COSO because of the frequency with which management of public companies are expected to use that framework for their assessments." If such is the case and AS2 and COSO are indeed closely interlinked,

60 Discussions with R. Malcolm Schwartz on February 15, 2006, at the IMA offices in Montvale, N.J.

61 Root, Steven. *Beyond COSO: Internal Control to Enhance Corporate Governance*. New York: John Wiley & Sons, 1998, p. ix.

then how does one explain the constant barrage of everyday complaints about the massive costs of implementing AS2? In reality, the fact is that in the absence of a generally accepted control assessment criteria for management, AS2 has become the de facto control standard that is used both by the management and the external auditors to assess the internal control system and form opinions on its effectiveness. This overemphasis on AS2 both by the internal auditors as well as management-types is also reflected when both groups also identify lack of practical guidance from the SEC on what exactly is a significant deficiency vs. material control weakness (See factor #5) as a major contributing factor to the high cost of compliance incurred by registrants.

Last, but not least, both groups of respondents also identified "external auditors' insistence on documenting and testing all processes irrespective of the residual risk profile of these processes" (factor #3) and "redundant testing performed by external auditors and internal auditors or SOX compliance group due to the inability of these groups to collaborate to reduce the sample size" (factor #6) as the two other major cost drivers for high SOX implementation costs. Various comment letters to the SEC, in response to its call for feedback on year-one implementation experiences along with the April 13, 2005, Roundtable, also provide a great deal of anecdotal evidence to support these findings.

To better understand the root cause of these perceived cost drivers, we interviewed a number of external auditors. These interviews revealed two facts that may be behind claims that the external auditing industry has engaged in over-auditing: One, the requirement "that, on an overall basis, *the auditor's own work must provide the principal evidence* for the [internal control] audit opinion,"[62] and two, "Management's assessment of the effectiveness of internal control over financial reporting is expressed at the level of *reasonable assurance*."[63]

The U.S. Chamber of Commerce, in defense of the external auditing industry, justifies over-auditing by stating that existing auditing standards do not provide sufficient guidance to the external auditors in determining when they have collected sufficient evidence or when enough is enough while auditing internal controls over financial reporting. In this respect it states that:

> Auditors must be allowed to exercise professional judgment, but the lack of specific guidance subjects them to substantial second guessing—by the plaintiffs' bar, the inspection staff of the PCAOB, and others—that their audits did not go far enough. Senior PCAOB officials have stated that they can't identify over-auditing. If the primary regulator doesn't know the outer limits of the standards, then how can audit firms or their clients be expected to?[64]

Related to the issue of excess costs, we also explored two other areas in this survey: (1) the extent to which the external auditors are conducting an integrated audit as defined by AS2 and (2) the extent of unnecessary documentation and testing done either by the company or its external auditors to reasonably conclude that a company has an effective system of internal control over financial reporting.

The issue of integrated audit is critical for various reasons. First, from a practical viewpoint,

62 See p. 18 of PCAOB Auditing Standard No. 2. Also see paragraphs 110 and 116 for more specific language on this requirement.
63 See paragraph 17 of PCAOB Auditing Standard No. 2.
64 "Auditing: A Profession at Risk." Washington D.C.: U.S. Chamber of Commerce, January 2006, pp. 14-15.

TABLE 12. STATUS OF THE INTEGRATED AUDIT

Extent of the Integrated Audit	# of Respondents (N=372)	% of the Total Sample	Small Companies (N=70)	Medium to Large Companies (N=302)
No Extent	29	7.8%	8.6%	7.6%
Some Extent	126	33.9%	30.0%	34.8%
Moderate Extent	93	25.0%	25.7%	24.8%
Large Extent	86	23.1%	18.6%	24.2%
Too Early to Tell	38	10.2%	17.1%	8.6%

Section 404(b) of the Sarbanes-Oxley Act of 2002 clearly states that an attestation by an external auditor under Section 404 should not be the subject of a separate engagement. The underlying intent of Congress in explicitly stating this is to direct the external auditors to avoid doing any duplicate work, control costs, and, perhaps even most importantly, capitalize on the understanding and knowledge they acquire about the effectiveness and holes in a client's internal control system and reflect that knowledge in the design and sample size of their tests. Paragraph E of AS2 states, "Each audit provides the auditor with information relevant to the auditor's evaluation of the results of the other audit." To ensure that a quality financial statement audit is conducted at a reasonable cost, SOX mandated that an auditor cannot conduct an evaluation of the internal control over financial reporting without conducting the related financial statement audit. Second, from a conceptual viewpoint, according to Bell, et al., a 21st Century public company audit or an integrated audit is a:

> process involving recursive planning and execution of audit procedures to enable triangulated[65] evidence-driven belief formation and revision and recursive risk assessments. Audit procedures, regardless of whether they are conducted during planning, control evaluation, substantive testing, or completion, are simply different and complementary kinds of risk assessment procedures…in the U.S. environment the PCAOB's issuance of AS2, which establishes the dual-opinion integrated audit, makes a significant turning point away from the compensatory view of the [Audit Risk Model] by increasing minimum standards dealing with auditors' need to obtain complementary forms of evidence.[66]

Thus, in an overall sense, the integrated nature of the audit mandated by Section 404 is more involved than the traditional audit and is directly related to the cost incurred by a registrant in complying with the requirements of Section 404.

Table 12 presents the results of our efforts to examine the extent to which external auditors

65 Note that according to the authors, "Triangulation occurs when the auditor understands the degree to which the same audit conclusion is supported by evidence of and from three fundamental sources…triangulation is a way of gathering mutually reinforcing evidence of and from three fundamental sources (entity business states, management business representations, and management information intermediaries) useful in formulating and revising well-justified beliefs by which auditors subsequently derive their risk assessments." See p. 27.

66 Bell, Timothy B., Mark E. Peecher, and Ira Solomon. *The 21st Century Public Company Audit: Conceptual Elements of KPMG's Global Audit Methodology.* Montvale, N.J.: KPMG International, 2005, p. 15.

TABLE 13. PERCENTAGE OF UNNECESSARY DOCUMENTATION AND TESTING

% of Unnecessary Documentation and Testing	# of Respondents (N=372)	% of the Total Sample	Small Companies (N=70)	Medium to Large Companies (N=302)
None	4	1.1%	1.4%	1.0%
<= 20%	95	25.6%	27.2%	25.1%
21%–40%	185	49.7%	42.8%	51.4%
41%–50%	45	12.1%	14.3%	11.6%
51%–75%	29	7.8%	8.6%	7.6%
> 75%	14	3.8%	5.7%	3.3%

are actually conducting an integrated audit as defined in AS2. Since only 19% of the small companies and 24% of the medium to large companies report integrated audits to a large extent, it is clear that the elusive goal of an integrated audit of internal control in conjunction with the financial statement audit is still far from a reality.

It is disappointing to note that a significant proportion of medium to large companies, which are most likely in year two of their Section 404 certification process, still feel that their external auditors are not really conducting an integrated audit (8% responded to no extent, and 35% responded to some extent). Slow progress toward the goal of the integrated audit is clearly reflected in the amount of unnecessary documentation and testing as reported by the survey participants in Table 13.

In much the same way as the cost of compliance is impacted by the integrated (or lack thereof) nature of the audit process, it is also impacted by the concept of reasonable assurance. Paragraph 17 of AS2 states that:

> Management's assessment of the effectiveness of internal control over financial reporting is expressed at the level of reasonable assurance....Reasonable assurance includes the understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance.

Similarly, the external auditor is also directed to focus his/her examination of the registrant's internal control system over financial reporting with the objective of providing reasonable assurance. Although "the prominence of this assertion...relates to the concern regarding accountability and liability,"[67] registrants have often complained that, at least during round one, the auditors not only carried out two disparate and simultaneous audits, but also, at a subconscious level due to fear of being second-guessed by the PCAOB inspectors, were truly looking to obtain absolute assurance from their clients. Undoubtedly, this contributed to the high cost of compliance. It is true that "no one

67 Root, Steven. *Beyond COSO: Internal Control to Enhance Corporate Governance*. New York: John Wiley & Sons, 1998, p. 139.

wants to be held accountable should subsequent events raise questions as to whether internal control was operating at the right level. [The concept of reasonable assurance] offers a basis for defending against allegations of wrongdoing, mismanagement, and the like."[68] Under AS2, however, the reality is that auditors are not limiting their legal risk in spite of engaging in over-auditing, as noted by the U.S. Chamber of Commerce in the report cited earlier.

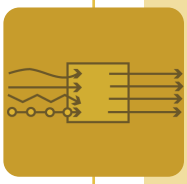
Table 13 presents the results to the question "What percentage of the documentation and testing, whether done by your organization or its external auditors, was unnecessary to reasonably conclude that your organization has an effective system of internal control over financial reporting?"

A review of the table suggests that for the overall sample, about one-quarter of the respondents felt that less than 20% of documentation and testing done by their company was unnecessary to reasonably conclude that they have an effective system of internal controls over financial reporting. A significant majority of the respondents (almost 62%) felt that the percentage of unnecessary documentation and testing was anywhere from 21% to 50%. Given that SOX compliance costs have run into millions of dollars for many companies, one can only speculate on the amount of potential "excess costs" in the system and consequently the loud outcry from the registrant community. When we analyze the sample by company-size subgroup, we find that almost 50% of the respondents from medium to large companies report that as high as 21% to 40% of the documentation and testing was unnecessary. Slightly more respondents from small companies (28.6%) than medium to large companies (22.5%) report the amount of unnecessary documentation and testing to be 41% or more.

Following are some of the written comments provided by the respondents regarding the cost drivers:

- Redundancies by external auditors are a significant factor. In year two, regarding application controls, this is a very significant factor as much time and money has been spent on excessive testing of application controls by our external auditors.
- We had most problems with the scope of work IT auditors felt they had to do to ensure that IT controls were adequate to ensure that our financial results were properly stated. It was almost as if they felt they had to perform a full-fledged IT General Controls Review when, in fact, not all IT controls directly impact the accuracy of our reported financial results. Still, identifying how much of the IT control environment needs to be examined is a tough issue. I think it would be helpful to look at actual problems with fraud or financial statements historically and identify which IT control weaknesses, if any, failed to better focus IT assessment and control testing activities. One shouldn't have to look at everything.
- Also contributing to increased costs was the lack of an efficient way to communicate results to the audit committee. We spent hours wrestling with Microsoft Word templates.
- Outside auditors tested far more than necessary despite internal audit work.
- In year one, our external auditors were not willing to place any reliance on work performed by corporate SOX group or Internal Audit, but insisted upon those groups collec-

68 *Ibid*.



tively performing as much testing as they did. This has changed in year two.

- The largest driver for excess costs associated with the year-one implementation was a lack of appropriate guidance for companies implementing the Act. All guidance was focused on the auditing firm's audit standards and the translation to what was then required by companies was varied, mercurial, and incomplete.
- The external auditors seemed very unwilling to rely on the work of internal audit despite a very adroit and well-credentialed internal audit team.
- We adopted a conservative approach to 302/404. When in doubt, the error was on the side of caution, and the procedure was identified as a control, documented, and tested. External auditors were highly conservative with respect to reliance on the work of others. As a result, we performed no work on their behalf.
- Internal Audit completed testing of controls without reliance on the work of the external auditors because management is charged to do that under the law. My interpretation is that they cannot delegate that responsibility to the external auditors. My thoughts are that the external auditors are NOT required to evaluate internal controls under SOX 404. They are required to do so because of the PCAOB rules. This requirement is driving up the costs. They should be charged only with attesting to management's evaluation as stated in the legislation.
- Delayed SEC/PCAOB guidance created an environment where the external auditor was running scared regarding shareholder actions if there were undetected errors in the audit that were surfaced later, etc.
- Current guidelines and application by an outside audit firm show little consideration towards the concept of efficiency.
- These questions hit the nail on the head. The COSO Framework is sound, but there is little to no definition on what satisfactorily defines test work (acceptable to the external auditors) and how to narrow the key controls to those that provide reasonable assurance (re: material misstatement or significant deficiency). There should be industry-wide standards or defined expectations from the external auditors. There is too much redundancy in effort—and again, the external auditors insist that independence of review requires that they retest the vast majority of test work. CSA is good, but process owners insist that they cannot test their own work—the role of management and supervision is now diluted. This used to be their role until audit defined it as a conflict. More guidance supporting CSA would be welcomed, but again it requires external audit approval or else the effort is in vain. It seems that the flow should be external audit tests key controls (that relate to residual risk and materiality), internal audit independently and randomly tests internal controls to continuously ascertain compliance (based on entity-wide risk assessment and in conjunction with operational audit priorities), and managers/supervisors monitor controls on a daily basis and assess their area of responsibility in an ongoing documented manner (perhaps a monthly CSA report).
- We experienced redundant testing as described in the last factor, and it was caused mostly by the inability of our external auditors to define what they considered to be adequate documentation, testing, etc. There was a tremendous amount of rework caused by changing guidance.

V.2.B. Risk-Based Assessment Approach

One of the points of contention that emerged during the April 13, 2005, SEC/PCAOB Roundtable had to do with the lack of a risk-based

assessment approach taken by the external auditors during the year-one implementation of SOX 404. Consequently, both the SEC and the PCAOB issued additional guidance, commonly referred to as the May 16 guidance. This guidance admonished the external auditors for excessive focus on detailed documentation and testing and for ignoring the top-down, risk-based approach to the audit of internal control:

> The feedback indicated that one reason why too many controls and processes were identified, documented, and tested was that in many cases neither a top-down nor a risk-based approach was effectively used. Rather the assessment became a mechanistic, check the box exercise. This was not the goal of the Section 404 rules, and a better way to view the exercise emphasizes the particular risks of individual companies. Indeed, an assessment of internal control that is too formulaic and/or so detailed as not to allow for a focus on risk may not fulfill the underlying purpose of the requirements. The desired approach should devote resources to the areas of greatest risk and avoid giving all significant accounts and related controls equal attention without regard to risk. [See page 4 of the SEC Guidance]

Similar concerns existed even prior to the enactment of the Sarbanes-Oxley Act of 2002. According to a July 1, 2002, article published in the California CPA, the authors contend that:

> There is an old saying in our business: CPAs love change, just not yet. Maybe that's why many have trouble embracing the changes proposed in the 1990's SAS 55, "Consideration of the Internal Control Structure in a Financial Statement Audit," and its successor, SAS 82, "Consideration of Fraud in a Financial Statement Audit." Both standards attempted to change the auditing industry by requiring auditors to consider inherent and control risk in audits and to rely less on a checklist approach. Unfortunately, both of these statements allow auditors to continue ignoring internal controls by choosing not to rely on them. Auditors remain in the comfort zone of the historical approach of assessing risk at maximum and doing across the board substantive tests. Twelve years after SAS 55, peer review results show that few auditors are performing risk-based audits. Instead, they are auditing areas with good internal controls because the controls are not documented, even though standards allow auditors to rely on undocumented internal controls.[69]

Given that the auditing industry extensively utilizes the Audit Risk Model (ARM) to minimize the overall audit risk by substituting the three compensatory components (i.e., inherent risk, control risk, and detection risk) of this model with each other,[70] it is not surprising that surveys (see, for example, the March 2005 FEI survey) indicate that most registrants favor a risk-based approach to the evaluation of their internal control system to comply with the SOX 404 requirements. What is not clear is whether each stakeholder (management, auditor, board, investor, etc.) shares a common view of what constitutes a risk-based audit and risk-based internal control assessment. To provide a context to understand the responses to the survey questions discussed later, it is important to first review the varied definitions of the risk-based audit that are prevalent in practice.

69 Scott, Thad, and Tom Noce. "So Long, Traditional Audit: No More 'Same As Last Year' with Risk-based Approach." *California CPA*. vol. 71, iss. 1, July 1, 2002.

70 See Bell, et al., 2005, for an excellent discussion in Chapter 2 of the Evolution of the Risk Assessment Orientation in Auditing.

It is believed that risk-based auditing debuted during the 1990s with the auditing industry's foray into offering high-margin internal auditing services. Recounting this history, Sobel observes:

> Risk-based auditing provided them with a compelling selling point. By starting with a thorough understanding of the business and its various business risks, auditors were able to make scope reductions that ensured key risks were addressed in the audit, without devoting valuable resources to other areas that had relatively lower risk.[71]

Without explicitly defining the term, Sobel moves on to define key characteristics of the risk-based audits:

- *Objective*: Determine the primary business risks and evaluate how effectively the controls and procedures are mitigating the risks to an acceptable level (i.e., how much residual risk remains).
- *Approach*: Understand the business, identify and evaluate the key business risks, and assess how effectively existing controls and procedures are mitigating these risks to an acceptable level. Controls and procedures relating to other risks (i.e., non-key risks) are not assessed in risk-based audits.
- *Focus*: Identify controls and procedures that are not operating effectively to mitigate the key business risks to an acceptable level.
- *Testing Approach*: Typically, a combination of substantive and compliance testing is utilized. The testing approaches used in both control-based and process-based auditing may be appropriate; however, testing will focus on key risks.
- *Recommendations*: Relate exceptions or errors to the key risks, and provide potential impacts of not effectively mitigating each risk to an acceptable level.[72]

Similarly, commenting on the superiority of the risk-based audits, Scott and Noce note:

> Risk-based auditing identifies inherently risky areas in a company and focuses only on those. Risk-based audits are not only more effective, but are more efficient because they reduce the problem of over-auditing. Risk-based audits…get you away from the frustrating practice of not relying on internal controls that the client already knows will work to prevent material misstatements. It also enables you to set-up or tighten controls in the client's risky areas.[73]

The above discussion suggests that risk-based auditing focuses on identifying and auditing high-risk areas in a company with the objective of rendering a most reliable audit opinion on the proprietary of the company's financial statements.

It is important to note, however, that not everyone has bought into the superiority of risk-based auditing. Consider the following statement in a *Wall Street Journal* article on the subject of risk-based auditing:

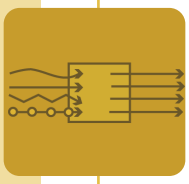
> In a September 2003 speech, Daniel Goelzer, a member of the Public Company Accounting Oversight Board, cautioned that the pressure to keep audit fees low had led major accounting firms to place more emphasis on "risk-based auditing," which he said had "contributed to the erosion of trust in auditing."[74]

71 Sobel, Paul J. *Auditor's Risk Management Guide: Integrating Auditing and ERM*. New York: Aspen Publishers, 2003, p. 3.05.

72 *Ibid*.

73 Scott and Noce, July 1, 2002.

74 Weil, Jonathan. "Tracking the Numbers, Outside Audit: Fannie Paid Little for Its Audits." *Wall Street Journal*. October 6, 2004, p. C1.



The same article continues, stating:

> Under this approach, auditors plan their work based on judgments about which clients are risky and which areas of a company's financial reports are most prone to error or fraud. Perceived low-risk areas of accounting, like cash on the balance sheet, often get just a cursory review; instead, auditors rely more heavily on what management tells them and data from the client's financial information systems. Perceived high-risk areas receive more attention. The problem, Mr. Goelzer cautioned, is that significant accounting problems may go unchecked if an auditor's judgments about risk prove incorrect.

Whether one agrees with the soundness of the approach as described above, it is clear that risk-based audits, to an extent, were used to reduce audit scope by the external auditors. And the assessment of what areas are risky was made by the external auditors either based on their own judgment or based on management's telling of what areas are risky in their business. No where in the above discussion of the risk-based audit approach is there any mention of focusing on the residual risk status information to understand the real risks to the reliability of the process that produces financial disclosures in a company?

Through a set of four survey questions, we set out to explore whether companies in our sample took a risk-based approach during their SOX 404 compliance initiative. However, as illustrated above, given that the understanding of what the term risk-based auditing means may not be uniformly understood and interpreted, we first defined for our survey participants what we believe—based on global risk management standards—is meant by the term risk-based approach to internal control assessment. We believe that to truly take a risk-based approach to internal control assessments, both management and the external auditors have to focus on the acceptability of the residual risk status. What separates our notion of risk-based approach from other commonly understood approaches is the emphasis not on perceptions (which can lead to more bad judgments on the part of the external auditor) but on the *quantitative measurement* of process error rate (or, conversely, the reliability of a process such as the financial reporting process) in all processes impacting a company's account and note disclosures. In other words, the hallmark of the residual-risk status approach is to emphasize the historical reliability of a registrant's financial reporting process, for example, as measured by the following residual risk status indicators:

- Indicator data (i.e., any known information about the effectiveness of controls);
- Impact data (i.e., how bad would the company's stock price or senior executives' compensation be impacted if there was an earnings shortfall);
- Impediment data (i.e., what problems, if any, stand in the way of an organization or a process owner adjusting the control portfolio to ensure that financial reporting for his/her span of control is reliable); and
- Concern data (i.e., any known information [or suspected problems] on potential threats to reliable financial reporting within the span of control of any process owner).

The first of the four questions asked the respondents about the type of risk-based approach their company took to comply with internal control certification requirements under Section 404. The specific question that was presented to the respondents was:

- Did your organization take a "risk-based" approach to its SOX compliance efforts? [By

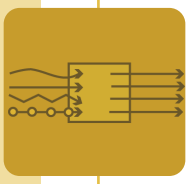
TABLE 14. TYPE OF RISK-BASED ASSESSMENT APPROACH

Type of Approach	# of Respondents (N=372)	% of the Total Sample	Small Companies (N=70)	Medium to Large Companies (N=302)
1. We took a risk-based approach in the way it is described in the question.	70	18.8%	14.3%	19.9%
2. We took a top-down, risk-based approach to define the scope of our work but did not identify or focus on the residual risk the way it is described in the question.	129	34.7%	32.9%	35.1%
3. We implemented a bottom-up approach by first documenting all processes and identifying all of the internal controls in the process, and then testing them exhaustively to conclude whether we have an effective system of internal control over financial reporting to certify under Sections 302/404.	136	36.6%	42.9%	35.1%
4. We did focus on the risks but not in the way the question describes it.	22	5.9%	8.6%	5.3%
5. Uncertain as to the approach that we took.	15	4.0%	1.4%	4.6%

risk-based approach, we mean focusing on the acceptability of the "residual risk status" of those business processes that most likely will result in control deficiencies based on historical error rates, etc.]

Table 14 presents the respondents' answers to this question.

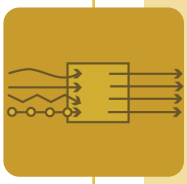
The results point to not-so-surprising findings. Only about 19% of the respondents believe that their companies took the risk-based approach to their internal control evaluations using the residual-risk status information. About 35% claim that they took the top-down, risk-based approach to scope their assessment work but without focusing on the residual-risk status or the real and potential error rate of their financial reporting processes or specific account and note disclosures. Almost 37% of respondents believe that their companies took the bottom-up approach and exhaustively documented and



tested all controls in all processes irrespective of their residual risk status profile. About 6% of respondents claim that their companies took the risk-based approach but in some different ways than the choices provided in our question. Interestingly, when we analyze our sample by company size, more small companies (almost 43%) are taking a bottom-up approach than the medium to large companies. Although it is not possible to provide any specific reason as to why smaller public companies are focusing more on a controls-oriented approach, we can only speculate that this may be due to lack of adequate risk and control training among the members of management and that because of the lower professional stature and influence of these firms with their external auditors.

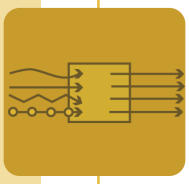
Below are some of the sample written comments made by respondents on the question of what type of risk-based approach they took to comply with SOX 404. These comments provide interesting insights into how companies are applying the concept of risk-based assessment at a more practical level:

- Our primary risk criteria were dollar value of account or number of transactions.
- We identified all major processes for all significant financial statement accounts. We then evaluated those processes for inherent risk as defined in COSO. We then identified the key controls that mitigated those risks.
- We performed a risk assessment to determine which portions of the business would need to be in scope for 404, and then which business cycles had the greatest financial reporting risk. We then identified the key controls in these cycles and tested these controls using a minimum annual sample rate provided by our external auditors.
- The external auditors drove this process resulting in an overreaching documentation and testing process.
- We started with a top-down approach, but it turned into more of a process-based approach as the project progressed.
- Due to lack of guidance, the bottom-up approach was used. In retrospect, if I knew what I know today, I would have taken a more integrative approach to it, but unfortunately guidance from PCAOB at the time we started was lacking, if at all defined.
- The bottom-up approach in year one of compliance has allowed us to take a significantly more risk-based approach in year two, resulting in a significant right-sizing of our efforts.
- We documented all processes and evaluated which items and entities to include for testing. Through discussion with external auditors, we decided which controls were key controls and how to reduce the number of controls that we thought were important, then focused on the ones that the company and the auditors agreed were key. We tested all key and some secondary/complimentary/contingent controls.
- We had already developed a self-assessment process (pre-SOX) and used that process to identify higher-risk areas as defined in 404.
- Auditors will not accept a risk-based approach due to lack of understanding and fear of the PCAOB.
- Difficult to explain to mid-level managers.
- We took a top-down, risk-based approach and then identified the residual risks, defining which and to what degree we should also evaluate the controls surrounding those risks.
- We evaluated inherent risks for each process, along with susceptibility to fraud, materiality, transaction volume, and level of objectivity in determining financial statement value, then focused efforts on those areas with more risk.
- Our approach used the COSO risks and made



sure our compensating controls covered these risks. We identified 13 major areas and selected the appropriate COSO risks.

- In year one, we did a bottom-up approach. In year two, we took a risk-based approach.
- In our view, the controls that reduce risk the most are the key controls that will be tested. If risk is not reduced substantially, it cannot be a key control, unless the control is necessary to break the threshold of acceptable residual risk.
- Risk was applied at the selection level of key control activities based on likely impact if a failure in operational effectiveness testing occurred during the year.
- Our external auditors seemed to be unwilling to take any other approach except for bottom-up. Consequently, the company had to take the same approach in order to get a clean opinion. This seems inefficient and inconsistent with what the PCAOB suggests.
- Totally disagree with your definition. The risk-based approach must focus on areas where there is at least a reasonable likelihood of a material error—not just any control deficiency. It also needs to start with inherent risk and prove through testing that residual risk is acceptable based on likelihood of a material error in future filings.
- We took a bottom-up approach for our first filing 6/2005. We found that most control failures at the process level were compensated for by analytics or entity-level controls. We are now reevaluating the identification of key controls to see if we can reduce reliance on process-level controls.
- Year-one documentation and testing was based more on coverage than risk. Year two was risk based.
- We looked at the risks and then defined key controls to mitigate the risks identified. Where there was or is residual risk, we had to or are evaluating if that residual risk is acceptable.
- All processes and controls were documented. Controls were tested for those routine processes that process 80% of the total transactions. Controls for all nonroutine and estimate processes were tested. In all tests, only key controls covering all assertions were tested.
- Heavy emphasis on entity-level controls. Top-down approach but extensive detailed documentation of processes and controls. Everything was tied to financial materiality and financial statement assertions (completeness, accuracy, etc.) vs. solely to residual risk.
- We also wanted to take a risk-based approach regarding the testing of the operating effectiveness of key controls, i.e., lower samples of testing in lower-risk processes. However, the external auditors have not agreed on this approach. All in-scope processes in their view should be tested to the same extent.
- Our approach in year one was both top-down and bottom-up (subsidiaries documented processes while the corporate level scoped materiality). In year two we took a top-down approach, however, we also began to assess our scope on a risk basis. Year three will continue to migrate more toward a risk-based approach.
- In year two we took a risk-based approach with respect to determining the extent of testing of reports and spreadsheets that are relied upon for completion of financial statement disclosures. That is, we used a risk-based approach to determine sample sizes for our baseline testing of systems and system-generated reports.
- We just completed year two of SOX compliance. In year one we took a bottom-up ap-



proach, and in year two we took a risk-based approach as you described it—focusing greater attention on the areas of residual risk. However, the external auditors still required test and recertification on virtually all of the key controls (regardless of level of risk).

- We implemented a bottom-up approach to documentation and control identification, then identified controls for testing using a risk-based approach, although not one that identified or focused on residual risk.
- In year two, we invested significant time in reengineering our efforts to focus only on key financial controls (vs. key and nonkey financial and operational controls in year one), which will give us an overall net reduction in internal efforts vs. year one. The process of identifying key controls to link to COSO-based control objectives allows us to prioritize our efforts and focus on the risks.
- We calculated an overall materiality and a planning materiality to use as a guideline to select our significant accounts to test.
- Much of the documentation prepared was procedural and not controls documentation. It ended up looking like a procedure manual.
- Top-down approach focus on materiality—after scope was set went back and assessed each in scope item for risk (impact and likelihood). Used the hindsight risk assessment to shape amount of direct detailed testing.
- We first documented all processes and identified risks and mitigating controls within these processes. We than tested the surrounding controls as they became available to test. In other words, we used a risk-based approach where and when it was possible. However, there were many revisions of documentation, which didn't allow us to test riskier areas until the end of the fiscal year.

We further explored our respondents' lack of focus on residual risk by asking the three specific questions listed in the left-hand column of Table 15. For each question, we asked our respondents the extent to which the SOX compliance team in their company identified plausible risks pertaining to financial statement accounts, note disclosures, and IT-related processes. Plausible risks are those risks that are most likely to occur given the history of the company and the environment (internal as well as external) in which it operates.

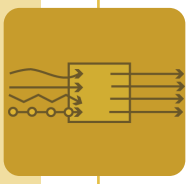
Table 15 summarizes the answers to each of these three questions. As far as identification of plausible risks is concerned, only 47% report that, to a large extent, their SOX compliance teams carried this step for financial statement accounts, and only 30% report that the same was done for the related note disclosures. What is more disturbing is that a significant percentage of the respondents report that their SOX compliance teams either did not identify or identified only to some extent the plausible risks that would threaten the integrity of the account balances in their financial statements (25%) and related note disclosures (37%). These findings are noteworthy. First of all, needless to say, note disclosures are an integral part of the overall financial disclosures package that help the reader understand the true financial position of the company. Inattention to the risks that could threaten the integrity of the information disclosed in each note disclosure would lead to significant information gaps, thereby reducing the reliability of all the financial disclosures made by the company in accordance with the SEC disclosure rules. Second, inattention to the plausible risks by a significant percentage of our respondents during their SOX 404 assessment confirms that the majority of the compa-

TABLE 15. DID THE SOX COMPLIANCE TEAM IDENTIFY PLAUSIBLE RISKS?

Question Statement	Extent to which Plausible Risks Identified (N=372)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. For the majority of your *financial statement accounts*, to what extent did your SOX 302/404 compliance team identify the plausible risks that could threaten the integrity of the balance in each one of the accounts?	4.6% (17)	20.7% (77)	25.0% (93)	47.3% (176)	2.4% (9)
2. For the majority of your *financial statement note disclosures*, to what extent did your SOX 302/404 compliance team identify the plausible risks that could threaten the integrity of the information in each one of the note disclosures?	8.3% (31)	29.0% (108)	26.3% (98)	30.1% (112)	6.25% (23)
3. To what extent did your SOX 302/404 compliance team identify plausible *IT-related* risks (e.g., infrastructure, access, integrity, security, etc.) for each application that impacts financial statement accounts and note disclosures?	1.6% (6)	18.0% (67)	25.0% (93)	53.5% (199)	1.9% (7)

nies are taking the control-centric and check-the-box approach to their management reporting on internal control. That is why the critics of this legislation, albeit incorrectly, are loudly proclaiming that SOX will not stop future Enrons or WorldComs. When it comes to the identification of IT-related plausible risks, the highest number of respondents (54%) report that their SOX compliance team carried this step. From these results, it is not clear to us as to why more SOX compliance teams would identify IT-related plausible risks than the plausible risks to account balances and related note disclosures.

Overall, these findings are not surprising given that AS2 mandates that to obtain an understanding of internal control over financial report-

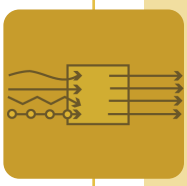


ing an auditor must determine the relevance of each of the five assertions[75] for each significant account. A cursory review of the definition of these assertions would suggest that it is possible that plausible risks (i.e., the risks that history has shown to occur) may be overlooked by management as well as the auditor during their evaluation of internal control because these assertions imply rather than explicitly state that attention should be given to all underlying risks while preparing financial disclosures.

Provided below are some of the written comments made by the respondents regarding identifying plausible risks related to the financial statement accounts, note disclosures, and IT processes:

- I think we could have done better focusing on risks. We talked about risk in general, but it did not have a big influence in the scope of our work.
- Our definition included anything with $1M of activity. This impacted the majority of our accounts and processes.
- Most accounts are reconciled monthly or quarterly. Tax accounts are the least subject to scrutiny and have the highest dollar impact if wrong.
- External auditors seemed to focus on all risks, whether plausible or not.
- Few issues found, but those that were did little to ensure the integrity of the financial statements. Some comments and recommendations, especially in respect to review and signoff, were considered extreme and basically useless in preventing fraud. The general feeling is that much of this will not prevent another Enron.
- Given the environment where external auditors were not commenting on acceptable risks or communicating anything, we were forced to identify any risk.
- There was very little emphasis put on what accounts could be negatively affected by a control weakness—many of our risks were related to documentation being signed. However, just because something is signed doesn't mean it's right.
- Plausible risks were addressed within the framework of the relevant financial statement assertions. For example, focus was primarily on which risk exists related to the financial statement assertion of completeness, or valuation, or validity, etc.
- Used assertions instead of risks—amount to the same thing.
- We used qualitative and quantitative formulas for each GL account and then across our business units.
- The relationship between financial statement accounts and the business processes triggering those accounts were identified, and, subsequently, entities were identified where these processes were deemed to be in scope for SOX 404 in order to achieve adequate coverage for the account.
- We used a scope document as a guide and reviewed accounts that would have or could

75 According to Paragraph 68 of AS2, the five assertions are: existence or occurrence, completeness, valuation or allocation, rights and obligations, and presentation and disclosure. AU section 326 defines each of these assertions as follows: Existence or occurrence: Whether assets or liabilities included in the financial statements exist at the balance sheet date and whether recorded transactions occurred during the period covered by the income statement; Completeness: Whether all transactions and accounts that should be in the financial statements are included; Rights and Obligations: Whether assets are rights of the entity and liabilities are obligations at a given date; Valuation or allocation: Whether asset, liability, revenue, and expense components are included in the financial statements at appropriate amounts; and Presentation and Disclosure: Whether components of financial statements are properly classified, described, and disclosed. Also see *Montgomery's Auditing*, 12th edition, pp. 6-2 to 6-3 for more detailed definitions of these assertions.



have had a material impact on our financial results when extrapolated.

- However, the initially defined key controls delve too deeply into internal control—and it is the defined key controls that external auditors are requiring to be tested. We need a better definition of key controls, and the external auditors need to provide that definition since they are the ones who give us a pass or fail. If we select and they disagree, we fail.
- The team documented their work procedures. Not much recognition of the risks involved.
- Our risk assessment process was better-defined and more granular than you suggest. The risk is to automated controls and undetected functionality that could result in material error, not just to applications without focus.

V.2.C. Use of COSO 1992 as the Control Evaluation Framework

To implement Section 404 of the Sarbanes-Oxley Act of 2002, the SEC amended Regulation S-K on August 14, 2003, to include Item 308. Under these SEC rules,[76] a registrant's annual report must include the following items [emphasis added]:

(a) Management's Annual Report on Internal Control over Financial Reporting: This report must contain

1. A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the registrant;
2. *A statement identifying the framework used by management to evaluate the effectiveness of the registrant's internal control over financial reporting;*
3. Management's assessment of the effectiveness of the registrant's internal control over financial reporting as of the end of the registrant's most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective;
4. A statement that the registered public accounting firm that audited financial statements included in the annual report containing the disclosure required by this item has issued an attestation report on management's assessment of the registrant's internal control over financial reporting.

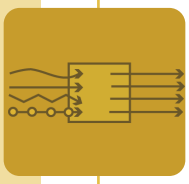
(b) Attestation Report of the Registered Public Accounting Firm: Provide the registered public accounting firm's attestation report on management's assessment of the registrant's internal control over financial reporting in the registrant's annual report containing the disclosure required by this item.

(c) Changes in Internal Control Over Financial Reporting: Disclose any changes in the registrant's internal control over financial reporting…that occurred during the registrant's fourth fiscal quarter in case of an annual report that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting.

In accordance with Item 308(a)(2), the PCAOB states in paragraphs 13 and 14 of AS2 that:

> Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework.…In the United States, the Committee of Sponsoring Organizations ("COSO") of the Treadway Commission has published *Internal Control—Integrated Framework*. Known as the COSO report, it provides a suitable and available framework for purposes of management's assessment.

76 See Regulation S-K Item 308(a)–(c).



This is consistent with the SEC Final Rule implementing Section 404. Based on these SEC and PCAOB endorsements, the COSO 1992 Framework has emerged as the primary control framework for companies of all sizes to assess and report on their internal controls.[77] In this section, we explore how the COSO 1992 Framework is being applied in practice to meet SOX requirements. This section is divided into three subsections: (1) Adoption of the COSO 1992 as the Control Evaluation Framework in the Pre-SOX Era, (2) Evaluation of the COSO 1992 Framework in light of the SEC criteria, and (3) Extent of Registrant Reliance on assessment guidance provided by the COSO 1992 Framework.

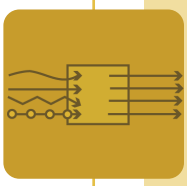
V.2.C.1. Reliance on COSO 1992 in the Pre-SOX Era

On the eve of his appointment as the COSO Board Chairman, Larry Rittenberg recalled the genesis of the Committee of the Sponsoring Organizations (COSO) and related it to today's events:

> COSO began in the mid-1980s when five private-sector organizations[78] that were concerned about the apparent increasing frequency of fraudulent financial reporting came together to sponsor the National Commission on Fraudulent Reporting—more commonly called the Treadway Commission after its chairman, James C. Treadway, Jr., a former SEC commissioner.
>
> The Treadway Commission conducted a comprehensive study of financial fraud in the United States and the factors that contributed to such fraud. It issued a detailed report in October 1987, consisting of 49 recommendations designed to enhance the prevention and detection of fraudulent financial reporting. These recommendations were directed at several relevant constituencies; public companies (20 recommendations); independent public accountants (9); the SEC and other regulators (12); and educators (8). These recommendations included a call for effective corporate internal control, objective internal audit functions, and informed oversight of financial reporting by effective audit committees. Interestingly, many of the original recommendations of the Treadway Commission now sound a lot like the Sarbanes-Oxley Act of 2002.
>
> Certainly the original Treadway Report in 1987 was a significant contribution. One of its most consequential recommendations was the development of a conceptual framework for implementing and evaluating internal controls. Prior to the 1992 issuance of COSO's *Internal Control—Integrated Framework*, internal control guidance consisted primarily of ad hoc checklists....Bill Ihlanfeldt, a former IMA chairman and former assistant controller at Shell Oil, played a key role in getting COSO to focus on internal control issues....Bill Bishop, a former IIA president, made sure the framework was broad enough to encompass controls

77 It is important to note, however, that in Section 404 Final Rule, the SEC makes it clear that "the final rules do not mandate use of a particular framework, such as the COSO Framework, in recognition of the fact that other evaluation standards exist outside of the United States, and that frameworks other than COSO may be developed within the United States in the future, that satisfy the intent of the statue without diminishing benefits to investors." Further, in footnote #67, the SEC elaborates on the other evaluation standards by indicating that the *Guidance on Assessing Control* published by the Canadian Institute of Chartered Accountants and the *Turnbull Report* published by the Institute of Chartered Accountants in England and Wales are examples of other suitable frameworks.

78 These five organizations are (1) the American Accounting Association (AAA), (2) the American Institute of Certified Public Accountants (AICPA), (3) The Financial Executives International (FEI), (4) The Institute of Internal Auditors (IIA), and (5) the Institute of Management Accountants (IMA).



comprehensively from an organizational perspective, not just a financial reporting point of view.[79]

At the time the SOX legislation was passed, the COSO 1992 Framework had been in existence for almost 10 years. There is no doubt that the issuance of the COSO 1992 Framework consolidated the then fragmented thinking on internal control in one place. And in terms of defining the principles of good internal control, COSO 1992 has stood the test of time. Whether organizations adopted the COSO 1992 Framework *en masse* or did the COSO 1992 Framework have any impact on their *thinking* or *behavior* in substantive ways is a debatable issue with strong opinions on both sides. For example, in a 1996 survey of 300 senior executives and 200 nonmanagement employees, Coopers & Lybrand (the author of the COSO 1992 Framework) found that almost four years after the issuance of COSO 1992:

- Only 10% of executives overall say they are aware of the Committee of Sponsoring Organizations' (COSO) model of risk controls. Not surprisingly, CFOs are much more likely than CEOs or mid-managers to say they are aware of the COSO model (19% vs. 7% and 4%). [See Finding #18, page xxi]
- Both CEOs and CFOs tend to be most critical of their companies' performance in assessing future risks with 36% and 40%, respectively, of each group saying their companies are doing an only fair or poor job (mid-managers=38%). [See Finding #4, page xii]
- Despite the nearly universal agreement that internal control is important across the various levels of management, 83% of CEOs, 65% of CFOs, and 82% of mid-managers agree that "making the numbers" is what really matters. [See Finding #2, page xi][80]

We are not aware of any other such surveys or research studies that document the usage or the effectiveness of COSO 1992 in the pre-SOX era. Based on the Coopers & Lybrand study, it appears that during the pre-SOX era, the use of the COSO 1992 Framework was very limited. Our field interviews, conducted as part of preparing the survey instrument for this research study, suggest that COSO 1992 was more of a philosophical treatise written by a group of accountants to draw the attention of the C-suite executives to the concept of internal control as a fundamentally sound business practice. It is important to mention here that COSO 1992 approaches internal control from a broader perspective rather than that envisioned by the drafters of Section 404.

When the Final Rules implementing Section 404 (as discussed at the beginning of II.C) ordained the COSO 1992 Framework to be the control framework for SOX 404 internal control certifications, COSO 1992 was suddenly back into the limelight. Since management reporting on internal control and auditor attestation of the same have always been contentious issues, and COSO 1992 has been available for use for nearly 15 years, we asked the survey participants the following three questions:

1. Prior to the enactment of the Sarbanes-Oxley Act of 2002, to what extent was *your organization* formally utilizing the guidance provided by the COSO 1992 Framework to effectively manage its enterprise risk and controls?

79 Tidrick, Donald E. "A Conversation with COSO Chairman Larry Rittenberg." *The CPA Journal*, November 2005.

80 Krane, Drake, and Joy Sever. *The Coopers & Lybrand Survey of Internal Control in Corporate America: A Report on What Corporations Are and Are Not Doing to Manage Risks*. New York: Louis Harris and Associates, 1996.

TABLE 16. USE OF THE COSO 1992 FRAMEWORK PRIOR TO SOX BY COMPANY MANAGEMENT

Response Scale	Q1: Extent to which COSO 1992 was utilized by our company to manage its enterprise risk and controls		
	Overall Sample (N=373)	Internal Auditors (N=146)	Management-types (N=227)
	% of Total	% of Total	% of Total
1. No Extent	37.8% (141)	45.9% (67)	32.6% (74)
2. Some Extent	31.4% (117)	30.1% (44)	32.2% (73)
3. Moderate Extent	13.9% (52)	11.6% (17)	15.4% (35)
4. Large Extent	11.3% (42)	7.5% (11)	13.7% (31)
5. Not Sure	5.6% (21)	4.8% (7)	6.2% (14)

2. Prior to the enactment of the Sarbanes-Oxley Act of 2002, to what extent were *your external auditors* formally utilizing the guidance provided by the COSO 1992 Framework to size-up the effectiveness of your entity's system of internal control and sharing their assessment annually with your company via the management letter?
3. Prior to the enactment of the Sarbanes-Oxley Act of 2002, to what extent was the *internal audit function in your organization* formally utilizing the guidance provided by the COSO 1992 Framework to size-up the effectiveness of your organization's system of internal control and sharing this assessment on a periodic basis with company management and the audit committee?

Our objective in asking these questions was to understand the extent to which the COSO 1992 Framework (or its thinking) had permeated the actual practice of assessing the internal controls in the pre-SOX era. Table 16 summarizes the results for question #1 for the overall sample as well as for the two subgroups: internal auditors and management-types.

It is noteworthy that only 8% of the internal auditors and 14% of the management-types report that their management team utilized COSO 1992, to a large extent, to effectively manage their organization's enterprise-wide risk and controls prior to SOX. Although according to the Coopers & Lybrand survey, "96% of all executives agree[d] that risk analysis is critical to an organization's success (96% CEOs and CFOs, and 97% of middle managers agree strongly or somewhat with this statement)," it is

TABLE 17. USE OF THE COSO 1992 FRAMEWORK PRIOR TO SOX BY EXTERNAL AUDITORS

Response Scale	Q2: Extent to which COSO 1992 was utilized by your external auditors to size up the effectiveness of your system of internal control and share this assessment annually with the company management		
	Overall Sample (N=373)	Internal Auditors (N=146)	Management-types (N=227)
	% of Total	% of Total	% of Total
1. No Extent	23.6% (88)	30.1% (44)	19.4% (44)
2. Some Extent	29.5% (110)	28.8% (42)	30.0% (68)
3. Moderate Extent	13.9% (52)	11.6% (17)	15.4% (35)
4. Large Extent	7.2% (27)	5.5% (8)	8.4% (19)
5. Not Sure	25.7% (96)	24.0% (35)	26.9% (61)

noteworthy that a large majority of them did not use the guidance provided in the COSO 1992 to conduct such assessments.[81]

Table 17 summarizes the results for question #2 for the overall sample as well as for the two subgroups.

Consistent with management's behavior, respondents indicate that in their opinion only a small number of external auditors (7.2%) were using the COSO 1992 Framework to a large extent to size-up their company's system of internal control and to report to their company's management their assessment or findings via the annual management letter. Given the large percentage of not sure responses (about 26%), it is plausible that few companies were even asking their external auditors for an assessment using COSO 1992. Overall, the findings presented in Table 17 suggest that the external auditing community, by and large, had banished internal control evaluations from its audit arsenal by setting the control risk to the maximum and totally relying on the analytical procedures and substantive testing, in the name of efficiency and to combat declining audit fees, to opine on the fairness of a client's financial disclosures.

Table 18 summarizes the results for question #3 for the overall sample as well as the two subgroups. The results indicate that although the use of the COSO 1992 Framework wasn't any better by the internal auditors (15%), it is clear that more internal auditing functions were using the COSO 1992 Framework in the pre-

81 Krane and Sever, 1996. See Finding #1.

TABLE 18. USE OF THE COSO 1992 FRAMEWORK PRIOR TO SOX BY INTERNAL AUDITORS

Response Scale	Q2: Extent to which COSO 1992 was utilized by your internal auditors to size up effectiveness of your system of internal control and share this assessment periodically with management and the audit committee		
	Overall Sample (N=373)	Internal Auditors (N=146)	Management-types (N=227)
	% of Total	% of Total	% of Total
1. No Extent	33.5% (125)	36.3% (53)	31.7% (72)
2. Some Extent	24.1% (90)	24.0% (35)	24.2% (55)
3. Moderate Extent	17.7% (66)	18.5% (27)	17.2% (39)
4. Large Extent	15.3% (57)	17.8% (26)	13.7% (31)
5. Not Sure	9.4% (35)	3.4% (5)	13.2% (30)

SOX era than management (11%) and the external auditors (7%).

We also analyzed responses to the three questions by company size. These results are presented in Table 19. A review of these findings indicates that a larger number of respondents from the smaller public companies report that their management, external auditors, and internal auditors utilized COSO 1992 to a much lesser extent[82] when compared with the responses from the medium to large companies' respondents.

82 This observation is based on combining the responses to the two choices of "no extent" and "some extent" for smaller vs. medium-to-large public companies for management (77.2% vs. 67.3%), external auditors (58.6% vs. 51.8%), and internal auditors (72.9% vs. 54.0%).

Our informal interviews with the external auditors, in the post-SOX era, confirm that a majority of external auditors still find it very difficult to determine when they have done enough to conclude whether all five components of the COSO 1992 Framework are operating effectively to conclude that the overall internal control system is effective.

Provided below are some of the written comments made by the respondents regarding the COSO 1992 Framework prior to the SOX requirements on internal control:

- The framework wasn't actively employed, but we were employing the principles.
- Internal Audit may have been using the COSO 1992 Framework to some extent, but man-

TABLE 19. USE OF THE COSO 1992 FRAMEWORK PRIOR TO SOX BY COMPANY SIZE

Response Scale	Use of COSO 1992 in a Small Company (N=70)			Use of COSO 1992 in a Medium to Large Company (N=303)		
	By Management	By External Auditor	By Internal Auditor	By Management	By External Auditor	By Internal Auditor
1. No Extent	54.3% (38)	25.7% (18)	54.3% (38)	34% (103)	23.1% (70)	28.7% (87)
2. Some Extent	22.9% (16)	32.9% (23)	18.6% (13)	33.3% (101)	28.7% (87)	25.4% (77)
3. Moderate Extent	14.3% (10)	12.9% (9)	10.0% (7)	13.9% (42)	14.2% (43)	19.5% (59)
4. Large Extent	5.7% (4)	4.3% (3)	10.0% (7)	12.5% (38)	7.9% (24)	16.5% (50)
5. Not Sure	2.9% (2)	24.3% (17)	7.1% (5)	6.3% (19)	26.1% (79)	9.9% (30)

agement in general was not aware of the framework.

- Key components of the COSO model were integrated into the business, but there was not a formal and detailed review of the financial control environment against the COSO Framework on a frequent and periodic basis.
- Limited to Internal Audit risk assessment for purposes of the audit plan.
- Partial use. Use was not documented but was practiced in some areas.
- We have always been very internal control-oriented, and SOX was more an exercise of documentation than it was implementing controls (they already existed). However, we did not necessarily formally follow COSO, just had good business practices already in place.
- The elements of the COSO Framework are self-evident and in a less formal manner were traditionally in place pre-SOX. Accounting has always had internal controls and monitoring of those controls—the control environment, tone at the top, and communication flow has always been one of providing accurate information with a strong sense of accountability and ethics. There is a better sense of risk assessment now that we have formally adopted COSO—and operationally the essence of it has been spread across the entire organization. It's a helpful tool to name COSO as our framework as that lends credibility to our efforts to those outside of our finance department.
- Control audits were usually performed on major scope audits only. Not all sections of the COSO risks were covered. Usually only payables, receiving functions, and appropriate balance sheet items. The following audit would concentrate on receivables, shipping functions, and appropriate balance sheet items.
- Tendency for external auditors has very much become to report as little as possible with regard to management letters, which for a

major part is caused by Section 404. They appear scared stiff to report anything, where we consider this added value to assist IAD in determining their future year's internal audit plan.

- Internal audit was a hit-or-miss process based on the individual judgment of the particular audit manager without any formal framework.
- We would review the risks every year and answer a quarterly questionnaire.
- We have utilized the components and elements outlined in COSO in the performance of our internal audit work. We do not formally follow the COSO guidance.
- Used portions of COSO, but not the full-blown model.

V.2.C.2. Suitability of the COSO 1992 Framework per SEC Criteria

The SEC Final Rules implementing Section 404 rightfully do not mandate the use of COSO 1992 or any other specific control-evaluation framework to rely upon as a benchmark to assess the effectiveness of a registrant's internal control over financial reporting. The Final Rules, however, do specify the suitability criteria that any framework must meet for it to be considered as an evaluation framework to satisfy the requirements under Section 404. According to the Section 404 Final Rule:

> A suitable framework must: be free from bias; permit reasonably consistent qualitative and quantitative measurements of a company's internal control; be sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal control are not omitted; and be relevant to an evaluation of internal control over financial reporting.

Given that these criteria form the litmus test for an acceptable evaluation standard, it would seem relevant to evaluate COSO 1992 against these criteria.[83] These results are produced in Table 20.

It is important to note that only about one-third (ranging from 34% to 40% for all four criteria) of our survey participants indicated that COSO 1992, to a large extent, meets the four criteria specified in the SEC Section 404 Final Rules. Similarly, another one-third of the survey respondents believe that COSO 1992 meets the SEC criteria to no extent or only to some extent. Almost 10% of the respondents are unable to evaluate the suitability of the COSO 1992 in light of the SEC criteria. Overall, the results presented in Table 20 are much less than desirable.

As mentioned earlier in Section II, there is increased sensitivity on the part of the lawmakers and the SEC related to the compliance costs being imposed on smaller public companies to comply with the requirements of Section 404. There is a general feeling in the SOX community that smaller companies are disproportionately impacted by the internal control requirements, and the application of COSO 1992 presents unique challenges to these companies because most of their internal controls are informal in nature.

To address these concerns, then-SEC Chairman William Donaldson appointed a Small Business

83 Our literature review did not reveal any empirical academic studies that have rigorously tested whether the COSO 1992 Framework meets the SEC suitability criteria. Academic researchers interested in internal control research can use experimental research techniques to study this important aspect of COSO 1992 or other global control models. We have initiated preliminary research in this area.

TABLE 20. PERCEPTIONS ABOUT COSO 1992 MEETING THE SEC CRITERIA OF SUITABILITY

Criteria for an Acceptable Control Evaluation Framework per Section 404 Final Rules	Extent to which COSO 1992 meets each one of the four criteria (N=301)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. Is free from bias	2% (7)	23% (68)	28% (85)	36% (108)	11% (33)
2. Permits reasonably consistent qualitative and quantitative measurements of a company's internal control over financial reporting	5% (15)	25% (74)	28% (85)	34% (102)	8% (25)
3. Is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal control over financial reporting are not omitted	3% (8)	25% (75)	27% (82)	36% (108)	9% (28)
4. Is relevant to an evaluation of internal control over financial reporting	2% (6)	22% (65)	27% (82)	40% (121)	9% (27)

Note: Percentages are rounded.

Advisory Task Force to review a whole host of issues impacting the smaller public companies, and Donald Nicolaisen, the SEC chief accountant at that time, asked the COSO committee to develop specifically tailored internal control guidance for the smaller public companies. In response to these demands by the SEC, the COSO board issued an exposure draft for public comment in October 2005.[84] The final three-volume Framework, *Internal Control over Financial Reporting—Guidance for Smaller Public Companies,* was released by the COSO Board in July 2006.[85]

Given the emphasis being placed on the needs of the smaller public companies, it is useful to understand whether the perceptions of the smaller public companies in our sample differ in any ways from the larger sample on the issue of the suitability of the COSO 1992 Framework to help them efficiently and effectively comply with Section 404. Table 21 presents these results by company size.

84 *Exposure Draft on Internal Control—Integrated Framework: Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting* issued by the Committee of the Sponsoring Organizations of the Treadway Commission, 2005.

85 *Internal Control over Financial Reporting—Guidance for Smaller Public Companies,* Volumes 1, 2, and 3 issued by the Committee of the Sponsoring Organizations of the Treadway Commission, July 2006. This document is available from www.cpa2biz.com.

TABLE 21. PERCEPTIONS ABOUT COSO 1992 MEETING THE SEC CRITERIA OF SUITABILITY BY COMPANY SIZE

Criteria for an Acceptable Control Evaluation Framework per Section 404 Final Rules	Extent to which COSO 1992 meets each one of the four criteria: Small Companies (N=59)			Medium to Large Companies (N=242)		
	No Extent to Some Extent	Moderate Extent	Large Extent	No Extent to Some Extent	Moderate Extent	Large Extent
1. Is free from bias	31% (18)	27% (16)	32% (19)	23% (57)	29% (69)	37% (89)
2. Permits reasonably consistent qualitative and quantitative measurements of a company's internal control over financial reporting	27% (16)	39% (23)	29% (17)	30% (73)	26% (62)	35% (85)
3. Is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal control over financial reporting are not omitted	29% (17)	29% (17)	37% (22)	28% (66)	27% (65)	36% (86)
4. Is relevant to an evaluation of internal control over financial reporting	19% (11)	44% (26)	32% (19)	25% (60)	23% (56)	42% (102)

Note: Percentages are rounded. Totals may not equal N because the table does not show the number of respondents choosing "Uncertain."

The results presented in Table 21 clearly indicate that fewer respondents from smaller companies perceive that to a large extent COSO 1992 meets the four specific criteria as laid out in the SEC Section 404 Final Rules. In other words, these response statistics suggest that smaller public companies have a less favorable impression of the COSO 1992 Framework than medium-to-large companies.

Since COSO 1992 is perceived to be "strongly influenced by the perspective of the independent accountants"[86] and thus too control-centric, it is plausible that internal auditors in our sample may have a more favorable impression of COSO 1992 when compared with the management-types. To test for this bias, we divided our response group into two subgroups: internal auditors and management-types. These results are presented in Table 22.

86 Root, 1998, p. 78.

TABLE 22. PERCEPTIONS ABOUT COSO 1992 MEETING THE SEC CRITERIA OF SUITABILITY BY JOB TITLE

Criteria for an Acceptable Control Evaluation Framework per Section 404 Final Rules	Extent to which COSO 1992 meets each one of the four criteria: Internal Auditor Responses (N=133)			Management-type Responses (N=168)		
	No Extent to Some Extent	Moderate Extent	Large Extent	No Extent to Some Extent	Moderate Extent	Large Extent
1. Is free from bias	22% (28)	29% (39)	41% (55)	28% (47)	27% (46)	32% (53)
2. Permits reasonably consistent qualitative and quantitative measurements of a company's internal control over financial reporting	29% (39)	32% (42)	35% (46)	30% (50)	26% (43)	33% (56)
3. Is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal control over financial reporting are not omitted	25% (33)	26% (35)	43% (57)	30% (50)	28% (47)	30% (51)
4. Is relevant to an evaluation of internal control over financial reporting	22% (30)	24% (32)	48% (64)	25% (41)	30% (50)	34% (57)

Note: Percentages are rounded. Totals may not equal N because the table does not show the number of respondents choosing "Uncertain."

As expected, more internal auditors (by a margin of almost 9% to 14% on criteria #1, #3, and #4, respectively) than management-types appear to believe that the COSO 1992 Framework meets the SEC criteria to a large extent. However, this difference of opinion between the two groups disappears when they are asked about criteria #2, which deals with the question of whether COSO 1992 permits, to a large extent, reasonably consistent measurements of a company's internal control over financial reporting (35% of internal auditors vs. 33% of management-types). This finding is noteworthy. If the underlying control model is unable to produce "reasonably consistent" conclusions about the effectiveness of a company's controls, tensions are bound to arise between management and external auditors on several issues, including whether enough control testing has been done to provide reasonable assurance. Unfortunately, based on the review of the last two years of comments filed with the SEC,

the implementation experience of numerous registrants confirms this suspicion.

Since criteria #2 is of paramount importance to producing apples-to-apples conclusions on control effectiveness, we further explored it by asking our respondents the following two questions:

1. In your opinion, using the COSO 1992 Control Framework, to what extent is it possible to arrive at a reliable pass or fail conclusion on the effectiveness of an entity's system of internal control over financial reporting (i.e., one that can be replicated by two independent assurance professionals within a narrow margin of error)?
2. In your opinion, using the COSO 1992 Control Framework, to what extent is it possible to achieve a *high level (90% or above) of consensus* between company management and their external auditors while opining on the effectiveness of a client's system of internal control under Sections 302/404 when each conducts its assessment on an independent basis?

The rationale to further explore criteria #2 is grounded in two main thoughts. First, since the registrants are now required to arrive at a binary (pass/fail) conclusion on the effectiveness of their internal control over financial reporting, it is important that COSO 1992 be able to facilitate such a conclusion, to a large extent, in a cost-effective way. Second, since the current requirements are for management and the external auditor to separately assess and opine on the effectiveness of a registrant's internal control over financial reporting, it is critical that, using the same set of facts, management as well as the external auditor be able to arrive at a similar conclusion with a much higher degree of consensus. If a control framework does not lead to a (1) *reliable pass or fail conclusion*, and (2) a *high degree of consensus* between managements' and auditors' assessments, then it does not meet criteria #2. It should be noted that we do not imply here 100% reliability or 100% consensus. Instead, what we believe the SEC rule intended was that any framework to become suitable for Section 404 purposes would lead to a sufficiently high degree of reliability and consensus in the assessment and opinion of the two groups.

The responses to the above-mentioned two questions are presented in Tables 23 and 24.

Table 23 indicates that only 22% of the overall respondents believe that it is possible, to a large extent, to arrive at a reliable pass/fail conclusion on the effectiveness of an entity's internal control over financial reporting. This meager support is again manifested when we divide our sample into smaller public companies (16%) and medium-to-large public companies (23%).

Similarly, when we examine Table 24, we find that only 18% of the overall respondents believe that it is possible to achieve, to a large extent, a high degree of consensus in the managements' and external auditors' assessment and opinion while using COSO 1992. When examined by company size, only 13% of the smaller public company respondents vs. 19% of the medium-to-large public company respondents believe that COSO 1992 results in a high degree of consensus.

Overall, the results presented in Tables 23 and 24 strongly complement and support the findings presented in Table 20. Together, these results raise major questions about COSO 1992 meeting the four criteria as laid out by

TABLE 23. IS IT POSSIBLE TO ARRIVE AT A RELIABLE PASS/FAIL CONCLUSION ON ICOFR USING COSO 1992?

Response Scale	# of Respondents (N=327)	% of the Total Sample	Small Companies (N=62)	Medium to Large Companies (N=265)
1. No Extent	8	2.4%	0.0%	3.0%
2. Some Extent	163	49.8%	58.1%	47.9%
3. Moderate Extent	59	18.0%	16.1%	18.5%
4. Large Extent	72	22.0%	16.1%	23.4%
5. Uncertain	25	7.6%	9.7%	7.2%

TABLE 24. CONSENSUS IN CONCLUSIONS BETWEEN MANAGEMENT AND EXTERNAL AUDITOR USING COSO 1992

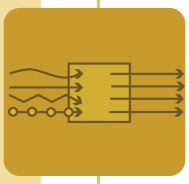
Response Scale	# of Respondents (N=327)	% of the Total Sample	Small Companies (N=62)	Medium to Large Companies (N=265)
1. No Extent	10	3.1%	1.6%	3.4%
2. Some Extent	166	50.8%	58.1%	49.1%
3. Moderate Extent	61	18.7%	19.4%	18.5%
4. Large Extent	58	17.7%	12.9%	18.9%
5. Uncertain	32	9.8%	8.1%	10.2%

the SEC in the Section 404 Final Rule.[87]

Provided below are the written comments made by our survey respondents as they relate to the above discussion:

- Limited usefulness in COSO framework.
- Minimum requirements on control environments were defined based on COSO. These can be used by the assurance professionals to define whether remediation is required. Note that we did not employ COSO for any transactional level controls. I don't know if IT (CobiT) will be discussed later, but a large degree of professional judgment remains necessary, regardless of structure and guidance we try to place around this (due to indirect relation between GITC and accounts).
- COSO as an assessment framework in conjunction with the definition of material weakness in AS2 allows a pass conclusion if there is an absence of a material weakness.

87 Some of the interviewees conjectured that since COSO 1992 was the only control framework available in the U.S. at the time of the issuance of Section 404 Final rules by the SEC, it is obvious that the Commission, in a rush to meet the deadlines imposed on it by the lawmakers, ordained the COSO 1992 Framework as meeting the requirements for Section 404 compliance but at the same time left the door open for better and robust frameworks to develop in the future.



- The issue is really more how the external audit firms interpret COSO. Although some firms are more conservative than others, they generally seem somewhat similar in their interpretations. I believe in my organization that two firms would probably come out the same way, but this is an easier conclusion to come to in a well-controlled organization. It might not be the same in an organization with internal control issues.
- COSO is only helpful to the extent it provides the general discussion of the interplay of the various components of the control environment. Very judgmental area, but believe disagreements are only in a few instances, re: existence of a material weakness.
- The framework is just that, a framework. What a company needs to do is work closely with their external auditor upfront and on an ongoing basis. We were lucky that the partner from our external audit firm wanted to cooperate. We did keep a wall between our two assessments, but we made sure that we agreed on risks and controls.
- It wasn't so much the framework as it was the agreement by management and internal and external audit to discuss and use the framework so we would all be on the same page, operating the same, coming up with the same (or pretty close) conclusions.
- It is still a framework, and the lack of experience applying it, both with external auditors as well as management, makes a number of interpretations of the framework subjective.
- As stated, the framework is sound but the definition of what's required to define the key controls and pass the test work is a failure.
- Limited usefulness in COSO framework.
- Worked well with external auditors but difficult with management.
- COSO helps to some degree as it provides a framework, but generally there will be interpretation issues and the shades of gray determination. If something is broken, then consensus is generally easy.
- The framework provides a reference point for management and the external auditors to evaluate the company controls, but there is a lot of opportunity for interpretation that could lead to disagreement.
- The only problem is when you have to determine whether you have a material deficiency. PCAOB is finally fleshing out AS2 relative to restatements and what is remote.
- It really gets down to who is on your account from the external audit firm. If they are reasonable, which we had, then you can get there.
- Active discussions between management and the external auditors on scope, materiality, testing approaches, significant accounts, and evaluation of magnitude and likelihood will ease differences between the two approaches. The 1992 COSO Framework, in and of itself, will not assist this process.
- We're all twisted up in our efforts—management now hires consultants (or an internal auditor) to do the work that external audit used to perform (but now in much greater detail and done by both). Management/supervision used to be a defined role with accountability for efficient, effective, accurate (work) and reporting. They still have that responsibility but now use separation of duty as an out—proclaiming that a second source must internally audit their work. External audit agrees, and we've looped back around to the double layering of audit on the same test work that is initially not performed, but supervised by management.

V.2.C.3. Reliance on COSO 1992 Assessment Guidance by Companies

For the purposes of the issues surveyed in this section, it is important to understand what is meant by internal control under COSO 1992.

> Internal control is a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
> - Effectiveness and efficiency of operations.
> - Reliability of financial reporting.
> - Compliance with applicable laws and regulations.[88]

In other words, the above definition suggests that the COSO 1992 Framework envisions internal control in a much broader sense than the notion of internal control over financial reporting as indicated in Section 404 and related SEC Final Rules. It is also important to note that internal control over financial reporting is subsumed within the above definition under the second objective.

Reviewing the history of the development of the COSO 1992 Framework, it appears that the scope of the term internal control as defined above was the result of a negotiation between the then COSO board members at the table. In this regard, Root notes that:

> One of the most basic objectives of the Framework was to develop a definition that could serve as the foundation for the balance of the document. This proved to be difficult due to the differing viewpoints that existed among interested parties. There were those who favored a broad definition in recognition of the view that internal control is inclusive of all, or virtually all, management undertakings. Others preferred a narrower definition that focused on internal control over financial reporting. Proponents of the broad concept prevailed. However, commentary was included that explicitly excepted certain management activities from internal control. Exclusions included entity-level objective setting, mission and values statements, strategic planning, risk management, and corrective actions. This compromise was directed at assuaging concerns that a broad definition would increase the risk of misleading external parties regarding management's ability to achieve all objectives associated with a broad definition. Thus, the Framework became influenced by liability considerations surrounding the issuance of reports on internal control to external parties, a largely voluntary practice among large public companies.[89]

When talking about the specific applicability of COSO 1992 for assessing internal control effectiveness, Root proclaims:

> After all, it's no secret that there really is no articulated internal control criteria in the COSO Framework. It provides only a broad definition consisting of three stated objectives, supplemented by a set of five internal control elements. Hence, there [is] ample room for guidance to aid anyone applying the Framework.

In the introduction to the evaluation tools module, the COSO Board states that:

> These evaluation tools are intended to provide guidance and assistance in evaluating internal control systems in relation to criteria for effective internal control set forth in the *Framework volume* of this report. Accordingly, users of these materials should be familiar with that volume.

88 *Internal Control—Integrated Framework*, 1992, p. 9.

89 Root, 1998, p. 117.

These tools are presented for *purely illustrative purposes*. They are not an integral part of the Framework, and their presentation here in no way suggests that all matters addressed in them need to be considered in evaluating an internal control system, or that all such matters must be present in order to conclude that a system is effective. Similarly, there is no suggestion that these tools are a preferred method to conduct and document an evaluation. Because facts and circumstances vary between entities and industries, evaluation methodologies and documentation techniques will also vary. Accordingly, entities may use different evaluation tools, or use other methodologies utilizing different evaluative techniques.[90]

The above caveat in the evaluation tools module that accompanies the Framework supports Root's assertion that the COSO 1992 Framework does not provide specific implementation guidance to actually carry out an internal control assessment engagement. This should not be construed to mean that we espouse a rules-based or a check-list oriented approach to internal control evaluations. COSO 1992 is not to be faulted for being broad and principles-based because, as discussed earlier, the need of the hour in the 1990s was to consolidate the fragmented thinking on internal control in one place in response to the Treadway Commission's Report on Fraudulent Financial Reporting. Today, however, the demand placed on the COSO 1992 Framework is to provide sufficient implementation guidance that registrants can use to cost-effectively conduct a top-down, risk-based control assessment so that they can legitimately claim that their internal control assessment/evaluation was conducted in accordance with [the COSO 1992's Internal Control-Integrated Framework].[91]

90 *Internal Control—Integrated Framework*, 1992, p. 1.

Since our review of the internal control certification in the SEC filings of the hundreds of registrants reveals that virtually everyone is claiming that they are conducting their internal control evaluations in accordance with COSO 1992, we asked survey respondents a series of questions to gauge the extent to which COSO 1992 provided these registrants practical or specific guidance while conducting their internal control evaluations. The first question, reproduced below, explored respondents' opinions on the level of the specific guidance provided by the COSO 1992 Framework:

- In your opinion, to what extent does the COSO 1992 Control Framework provide *specific* guidance (as opposed to motherhood and apple-pie type of guidance on elements of an internal control system) to all those who are responsible for assessing and concluding on the effectiveness of a company's system of internal control over financial reporting?

The results for this question are presented in Table 25.

Only 4% of the overall survey respondents believe that COSO 1992 provides them, to a large extent, with any specific guidance in assessing and concluding the effectiveness of internal control over financial reporting. About 16% even go to the extent of claiming that it does not provide them with any guidance with respect to their internal control evaluation. The majority of the respondents (almost 76%) are willing to give credit to COSO 1992 only to some or a moderate extent.

91 See Part II.B.2.a of the Section 404 SEC Final Rule. Recall that the SEC Final Rule implementing Section 404 does not name any specific control evaluation framework but clearly states that "COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements."

TABLE 25. LEVEL OF SPECIFIC IMPLEMENTATION GUIDANCE PROVIDED BY COSO 1992

Response Scale	# of Respondents (N=327)	% of the Total Sample	Internal Auditors (N=137)	Management-types (N=190)
1. No Extent	53	16.2%	16.1%	16.3%
2. Some Extent	173	52.9%	56.2%	50.5%
3. Moderate Extent	75	22.9%	24.1%	22.1%
4. Large Extent	12	3.7%	2.2%	4.7%
5. Uncertain	14	4.3%	1.5%	6.3%

There is no difference in the perceptions of our respondents on this question linked to company size. In other words, medium-to-large companies do not respond to this question any more favorably than the smaller companies. However, contrary to the expectations, as reported in Table 25, an even smaller number of internal auditors (2.2%) believe the COSO 1992 Framework provides, to a large extent, any detailed guidance. Overall, these results should not come as a surprise to anyone. The earlier discussion has already established that the original authors of COSO 1992 did not develop the framework with the goal of providing specific and detailed guidance for potential pass/fail conclusions on internal control effectiveness.

In light of the fact that COSO 1992 was never intended to be used for pass/fail control assessment, what does a registrant and its external auditor do under such circumstances? According to Chan, et al.:

> Consequently in practice, during the first-year implementation, a great majority of the companies and their external auditors adopted a two-prong approach to the evaluation of an entity's system of internal control. A typical internal control assessment involved evaluating only entity-wide controls using the five COSO categories. The process and activity level controls were evaluated according to the guidance provided in AS2 along the dimensions of "more than inconsequential" and "more than remote." If the later assessment discovered a material control weakness, it was concluded that the client's system of internal control [over financial reporting] is ineffective. This approach to the control assessment highlights the inability of the COSO 1992 Framework in providing company managements with a defensible benchmark that they can use to reliably and consistently conclude whether their system of internal control is effective. Furthermore, the irony of this approach is that U.S.-listed companies continue to claim that they are conducting their internal control assessments using the COSO 1992 control model, while in reality it is AS2 that dominates the control assessment process to arrive at SOX 302/404 opinions.[92]

To further understand the extent to which AS2 marginalizes the broader-level guidance provided in COSO 1992, we asked our respondents whether it is possible for them to arrive at a

92 Chan, et al., 2006, p. 26.

TABLE 26. CAN COSO 1992 GUIDANCE ALONE LEAD TO A PASS/FAIL CONCLUSION?

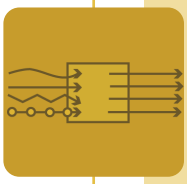
Response Scale	# of Respondents (N=301)	% of the Total Sample	Internal Auditors (N=133)	Management-types (N=168)
1. No Extent	44	14.6%	14.3%	14.9%
2. Some Extent	128	42.5%	41.4%	43.5%
3. Moderate Extent	74	24.6%	24.1%	25.0%
4. Large Extent	38	12.6%	16.5%	9.5%
5. Uncertain	17	5.6%	3.8%	7.1%

pass/fail conclusion on the effectiveness of their internal control over financial reporting in the absence of guidance provided in AS2. The specific question is reproduced below and the results appear in Table 26:

- The SEC's Final Rules implementing Section 404 state, "Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the registrant's internal control over financial reporting." AS2 requires the same conclusion from the external auditors. In other words, this requirement essentially sets the pass/fail criteria. In the absence of such a specific requirement, in your opinion, to what extent is it possible for management as well as external auditors to form a pass/fail opinion on the effectiveness of internal control over financial reporting solely based on the guidance provided in the COSO 1992 Framework?

The results presented in Table 26 indicate that only 13% of all respondents believe that, to a large extent, it is possible to arrive at a binary (pass/fail) conclusion using the guidance provided by the COSO 1992 in the absence of AS2. Interestingly, just about the same percentage of respondents (15%) believes that it is not at all possible. Leaving out the ones who are uncertain about the suitability of COSO 1992 to provide such guidance, almost two-thirds of our sample respondents believe that such a pass/fail conclusion is possible only to some or a moderate extent under COSO 1992 guidance.

The distribution of these results does not substantially change when we analyze our sample either by company size or job title. These findings further reinforce the results reported in Table 25, which concluded that the COSO 1992 Framework provides guidance that is good from a broader perspective but does not provide registrants and auditors enough focus in assessing and reporting on internal control to conclude that their assessment was truly done in accordance with COSO 1992's *Internal Control—Integrated Framework*. At this point, it would also be pertinent to mention that when asked "in your opinion, which one of the following two statements is 'more true' for your first-year SOX certification efforts," almost 62% of the respondents chose the statement that the *majority of their internal control assessment was largely guided by and conducted in accordance with the PCAOB Auditing Standard #2 as*



opposed to in accordance with COSO 1992's Internal Control—Integrated Framework.

We also asked our respondents the extent to which their SOX compliance team, at the entity level, evaluated the overall effectiveness of each one of the five main COSO components as part of the process used to form an opinion on the effectiveness of internal control. Only about 35% of the respondents answered this question to a *large extent*. There was an even split (about 28% each) between the two choices of to some extent and to moderate extent. These responses are consistent with the findings reported above and reinforce the dominance of AS2's guidance in assessing and evaluating internal control over financial reporting.

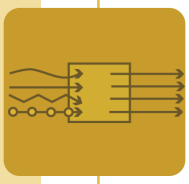
Provided below are the written comments made by our survey respondents as they relate to the above discussion:

Table 25-Related Comments

- COSO is very vague and nonspecific. Even the training classes in COSO cannot answer the what-to-do questions asked by auditors.
- The general guidance is there. The problems occur in the use of appropriate judgment to determine whether there is truly a problem or not. Because there is judgment involved, conflict arises with the external auditors.
- It was too high level. Not enough detail causing much confusion and caused a lot of unnecessary money to be spent in the interpretation.
- Specific insight is provided regarding company-level controls (tone at the top, risk assessment, oversight, etc.) more so than process-level/transactional-level controls.
- I think the overarching framework needs to be broad. I think the detailed testing needs to be more focused. By more focused, I think the testing should be based on experience (a) in particular industries and be (b) actual problems with fraudulent or materially inaccurate financial reporting.
- The 1992 COSO Framework requires a substantial amount of judgment when determining what level of framework application is appropriate in smaller- and mid-sized entities. Because judgment is subjective, it is difficult to achieve consistent opinions as to the adequacy of the implementation.
- The framework provides only general guidance that requires significant interpretation.
- Highly conceptual. Needs interpretation and training. Certainly not an out-of-the-box framework.
- Subjective items especially in areas such as control environment, where it is difficult to measure, COSO was not a tremendous help.
- It is practical and logical. The design of controls is adequately supported. The testing elements of Sarbanes 404 are not so well supported by COSO written guidance—other guidance is sufficient, however.

Table 26-Related Comments

- This would be very difficult without the pass/fail criteria.
- There is some ego involved; management does not want to publicly state that the organization they are responsible for does not have an effective control environment. Without strict guidance (requirements), management would tend to be liberal in their assessment and focus on getting comfortable evaluating controls as effective.
- Difficult using only COSO because usually auditors speak in terms of quantifiable materiality.
- COSO alone could not lead one to a pass/fail-type conclusion.
- COSO provides the framework or model for a



system of internal accounting controls but does not provide guidelines or criteria in evaluating internal controls.

- Depending upon the pass/fail criteria this will not usually be clear and straightforward. The external auditors sometimes try to make everyone fall into a few different categories even when this is not reasonable. This is the toughest area about a strict pass/fail test.
- While COSO was the framework, it really was the PCAOB guidance (AS2) and discussions with management, internal and external audit that helped us to conclude.
- But the condition is that focus is not only on the COSO objective financial reporting, which it currently is, but also on efficiency of operations and compliance with laws and regulations. In that respect the current requirements provide a fake assurance for the investors in my opinion.
- Cannot solely base it on COSO—you can never replace experience and professional judgment. COSO won't tell you how to classify it.

In the following subsections, we explore the relevance of guidance provided by COSO 1992 in the following four categories: (1) assessment of specific account balances and note disclosures, (2) assessment of fraud risk factors, (3) assessment of IT controls, and (4) mapping of internal control weaknesses to COSO components.

V.2.C.3.a Assessing Account Balances and Note Disclosures Using COSO 1992

The COSO 1992 Framework describes the five components of internal control as follows:

> Internal control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. The components are:
>
> *Control Environment*—The core of any business is its people—their individual attributes, including integrity, ethical values and competence—and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.
>
> *Risk Assessment*—The entity must be aware of and deal with the risks it faces. It must set objectives, integrated with the sales, production, marketing, financial, and other activities so that the organization is operating in concert. It also must establish mechanisms to identify, analyze, and manage the related risks.
>
> *Control Activities*—Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's objectives are effectively carried out.
>
> *Information and Communication*—Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange the information needed to conduct, manage, and control its components.
>
> *Monitoring*—The entire process must be monitored and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.[93]

93 *Internal Control—Integrated Framework: Evaluation Tools.* Jersey City, N.J.: COSO, September 1992, pp. 13–14.

TABLE 27. RELIANCE ON FIVE COSO 1992 COMPONENTS TO EVALUATE CONTROLS FOR SPECIFIC ACCOUNT BALANCES

Five Components of the COSO 1992 Framework	Extent to which your SOX Compliance Team Relied on Five COSO Components while Evaluating Internal Controls over Specific Account Balances (N=327)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. Control Environment	6% (20)	28% (91)	31% (102)	31% (102)	4% (12)
2. Risk Assessment	7% (23)	32% (106)	34% (111)	23% (75)	4% (12)
3. Control Activities	4% (12)	23% (75)	30% (99)	39% (129)	4% (12)
4. Information and Communication	7% (23)	36% (119)	28% (93)	23% (74)	6% (18)
5. Monitoring	6% (21)	31% (101)	31% (102)	27% (89)	4% (14)

Note: Percentages are rounded.

In this subsection, we further explore the extent to which our survey respondents relied on the guidance provided by COSO 1992 for each one of the five main COSO control components when evaluating internal control over specific account balances. To understand this, we asked the following question:

- When evaluating internal controls related to most of your *specific account balances* to what extent did your SOX compliance team specifically rely on the guidance provided by the COSO 1992 Framework for each one of the five COSO components of internal control?

Table 27 presents the responses to this question. The results suggest that only 23% to 39% of the respondents believe that one or more of COSO's five elements provided them, to a large extent, with specific guidance while evaluating internal controls related to their company's specific account balances. The *control activities* element appears to be cited by most respondents (39%) and the *risk assessment* and *information and communication elements* are each cited by only 23% of the respondents. Given that 47% of the respondents (see Table 15) claimed that their SOX compliance team identified plausible risks for the majority of their financial statement accounts, these findings indicate that a significant number of respondents carried out this risk-identification activity without regard to the guidance provided in this component of the COSO 1992 Framework.

When we analyze our sample by subgroups, some additional insights emerge. Tables 28 and 29 summarize these results. It is important to note that 45% of the internal auditors as compared with 36% of the management-

TABLE 28. RELIANCE ON FIVE COSO 1992 COMPONENTS TO EVALUATE CONTROLS FOR SPECIFIC ACCOUNT BALANCES BY JOB TITLE

Five Components of the COSO 1992 Framework	Extent to which your SOX Compliance Team Relied on Five COSO Components while Evaluating Internal Controls over Specific Account Balances (N=327)					
	Internal Auditor Responses (N=137)			Management-type Responses (N=190)		
	No Extent to Some Extent	Moderate Extent	Large Extent	No Extent to Some Extent	Moderate Extent	Large Extent
1. Control Environment	33% (44)	34% (46)	33% (45)	35% (67)	29% (56)	30% (57)
2. Risk Assessment	43% (60)	38% (52)	18% (24)	36% (69)	31% (59)	27% (51)
3. Control Activities	22% (30)	33% (45)	45% (61)	30% (57)	28% (54)	36% (68)
4. Information and Communications	43% (62)	31% (43)	21% (29)	42% (80)	26% (50)	24% (45)
5. Monitoring	35% (48)	34% (47)	29% (40)	39% (74)	29% (55)	26% (49)

Note: Percentages are rounded. Totals may not equal N because the table does not show the number of respondents choosing "Uncertain."

types relied, to a large extent, on guidance provided by the control activities component of COSO 1992 while they evaluated internal control over specific account balances. Similarly, more management-types (27%) relied on the risk-assessment component than the internal auditors (18%). Surprisingly, the information and communication and monitoring components either were not relied upon or relied only to some extent by both the groups. Table 29 presents the same results by company size. A review of this table indicates that a larger percentage of respondents from medium-to-large companies believe that their SOX compliance teams relied on the five COSO components only to some extent when evaluating their internal controls over specific account balances.

Here are the written comments made by our survey respondents as they relate to the discussion:

- The COSO components were included in our documentation but to be honest most of the documentation team did not know how to apply them practically. They were just there because the auditors were expecting to see some words around each area.
- My impression was that our corporation and external auditors chose the account balances based on materiality to our overall corporation's financial statements. I don't believe COSO was a critical or direct input.
- We were way too focused on control activities, in my opinion.
- At account level we focused primarily on

TABLE 29. RELIANCE ON FIVE COSO 1992 COMPONENTS TO EVALUATE CONTROLS FOR SPECIFIC ACCOUNT BALANCES BY COMPANY SIZE

Five Elements of the COSO 1992 Framework	Extent to which your SOX Compliance Team Relied on Five COSO Components while Evaluating Internal Controls over Specific Account Balances					
	Small Company Responses (N=62)			Medium to Large Company Responses (N=265)		
	No Extent to Some Extent	Moderate Extent	Large Extent	No Extent to Some Extent	Moderate Extent	Large Extent
1. Control Environment	37% (23)	24% (15)	35% (22)	33% (88)	33% (87)	30% (80)
2. Risk Assessment	37% (23)	35% (22)	24% (15)	40% (106)	34% (89)	23% (60)
3. Control Activities	29% (18)	34% (21)	34% (21)	26% (69)	29% (77)	22% (58)
4. Information and Communications	45% (28)	26% (16)	26% (16)	43% (114)	29% (77)	22% (58)
5. Monitoring	40% (25)	26% (16)	31% (19)	37% (97)	32% (86)	26% (70)

Note: Percentages are rounded. Totals may not equal N because the table does not show the number of respondents choosing "Uncertain."

financial statement assertions.

- We adopted the format to reflect the tangible elements that addresses the approximate 67 points of focus enunciated in the document framework.
- They did rely on some elements but they didn't exclusively rely on it, and they didn't narrow their key controls or test work based on it because they were afraid to do so (i.e., external audit might result in a fail). Ironically, the external audit team also used the COSO framework but still tested all of the key controls without truly assessing the significance of those controls.
- Used typical process-based controls (purchasing cycle, payroll cycle) and practice aids showing subprocesses within these processes, sample control activities, etc. Control activities is where COSO comes up short, I think.
- For control activities, the compliance team was obliged to follow the control framework provided by our external auditors.

We asked the same question of our respondents with regard to the note disclosures made in their financial statements. This question is:

- When evaluating internal controls related to most of your note disclosures, to what extent did your SOX compliance team specifically rely on the guidance provided by the COSO 1992 Framework for each one of the five COSO components of internal control?

TABLE 30. RELIANCE ON FIVE COSO 1992 COMPONENTS TO EVALUATE CONTROLS ON NOTE DISCLOSURES

Five Components of the COSO 1992 Framework	Extent to which your SOX Compliance Team Relied on Five COSO Components while Evaluating Internal Controls over Note Disclosures (N=327)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. Control Environment	11% (37)	31% (100)	25% (81)	19% (62)	14% (47)
2. Risk Assessment	13% (43)	33% (107)	24% (77)	16% (53)	14% (47)
3. Control Activities	10% (33)	28% (92)	24% (80)	23% (76)	14% (46)
4. Information and Communication	14% (46)	30% (97)	24% (80)	17% (55)	15% (49)
5. Monitoring	14% (45)	31% (101)	25% (81)	16% (52)	15% (48)

Note: Percentages are rounded.

Table 30 summarizes these responses. These findings indicate that, across the board, only 16% to 23% of the respondents believe that their SOX compliance teams relied on the guidance provided by the five COSO components while evaluating internal controls over their company's note disclosures. Almost 10% to 14% claim no reliance on the five COSO components, with about 15% being uncertain on whether any reliance was placed on the five COSO components. These results do not substantially change when we analyze our sample in subgroups either by company size or job title.

Overall, the results presented in Tables 27–30 suggest that a significant majority of our respondents did not use, to a large extent, the guidance provided in the five COSO components while evaluating effectiveness of internal controls over their account balances and related note disclosures. These findings squarely contradict the statements made by SEC registrants in their public filings that they conducted their internal control assessment in accordance with COSO 1992's *Internal Control—Integrated Framework*.

V.2.C.3.b. Assessing Fraud Risk Vulnerability Using COSO 1992

Paragraphs 24–26 of the PCAOB Auditing Standard No. 2 and the related SEC rules implementing Section 404 specify management's and external auditor's responsibility for fraud risk and control assessment. In addition to the specific requirements cited in AS2, the external auditor is also required to conduct his/her evaluation of fraud risk controls consistent with SAS 82, *Consideration of Fraud in a Financial Statement Audit*. Collectively these requirements suggest that management as well

TABLE 31. ASSESSMENT OF FRAUD RISK FACTORS

Response Category	Did you complete an antifraud assessment for industry-specific risk factors? (See SAS 82 category (b)) (N=327)	Did you evaluate macro-level antifraud controls other than industry-risk factors? (See SAS 82 categories (a) and (c)) (N=324)
Yes	73.4% (240)	69.1% (224)
No	26.6% (87)	30.9% (100)

as the external auditor must complete an assessment of controls designed to prevent, identify, and detect fraud-related risks that could result in unreliable financial disclosures. SAS 82, paragraph 16, groups the risk factors that relate to misstatements arising from fraudulent financial reporting into three distinct categories:

a. *Management's characteristics and influence over the control environment*. These pertain to management's abilities, pressures, style and attitude relating to internal control and the financial reporting process;
b. *Industry conditions.* These involve the economic and regulatory environment in which the entity operates; and
c. *Operating characteristics and financial stability.* These pertain to the nature and complexity of the entity and its transactions, the entity's financial condition, and its profitability.[94]

These categories suggest that a common-sense approach to assessing fraud vulnerability would start with an assessment of macro-level anti-fraud controls as well as anti-fraud assessment for industry-specific risk factors that would lead to fraudulent financial reporting. Consequently, we asked our survey respondents whether they evaluated macro-level antifraud controls and antifraud controls for industry-specific risk factors while assessing their internal control over financial reporting. If they answered yes to these questions, we further probed them by asking the extent to which they relied upon the guidance provided to them in the five COSO components to carry out these antifraud assessments.

Table 31 presents the results for the fraud assessment at the macro-level as well as for the industry-specific risk factors. The results present a disturbing picture. Almost 27% of the respondents believe that their SOX compliance team did not assess controls for industry-specific fraud risk factors as mentioned in category (b) per SAS 82. Similarly, about 31% of the respondents reported that they did not perform a macro-level antifraud assessment for fraud risk factors as they relate to categories (a) and (c) per SAS 82. The reason we separately asked the question with respect to the industry-specific risk factors is due to the fact that the genesis of the financial fraud in recent scandals such as Enron, WorldCom, and Global Crossing, etc., was rooted in deteriorating industry conditions.

94 Paragraph 17 provides numerous examples of risk factors to fraudulent financial reporting in all of the three categories.

TABLE 32. ASSESSMENT OF FRAUD RISK FACTORS BY COMPANY SIZE

Question Statement	Small Companies (N=62)		Medium to Large Companies (N=265)	
	Yes	No	Yes	No
1. Did you complete an antifraud assessment for industry-specific risk factors?	66.1% (41)	33.9% (21)	75.1% (199)	24.9% (66)
2. Did you evaluate macro-level antifraud controls other than industry-risk factors?	67.7% (42)	32.3% (20)	69.5%* (182)	30.5%* (80)

*Three respondents did not answer this question.

Table 32 analyzes the survey responses by company size. What we find is that a fewer number of smaller public companies conducted fraud risk assessments, both at the macro-level (68%) as well as for industry-specific risk factors (66%), when compared with the medium-to-large companies (70% and 75%, respectively). This is an important finding in light of the fact that "a 1999 report commissioned by the organizations that sponsored the Treadway Commission found that the incidence of financial fraud was greater in smaller companies."[95] This finding also calls into question the validity of the arguments advanced by many of the smaller public company lobby groups asking for exemption from Section 404 requirements.

For each one of the two fraud-risk assessments discussed above, we also asked our survey respondents (only the ones who answered yes to the two questions presented in Tables 31 and 32) the extent to which they relied on the guidance provided by each one of the five COSO 1992 components of internal control.

The results presented in Table 33 indicate that less than 30% (from 20% to 29%) of the respondents believe that their SOX compliance team relied, to a large extent, on the guidance provided by the five COSO 1992 components when completing their company's antifraud assessment for industry-risk factors. Almost 10% of the respondents answered a flat no, indicating that they did not rely on the guidance provided by the five COSO 1992 components, and about 15% of the respondents reported being uncertain about whether their SOX compliance team relied on any such guidance while conducting antifraud assessment for their company's industry-specific risk factors.

These results do not improve substantially when survey respondents are asked the same question but this time with respect to the assessment of the macro-level fraud risk factors. These findings are presented in Table 34.

The results presented in Tables 33 and 34 call into question whether the COSO 1992 Framework "is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company's internal

95 See Section E: Agency Action to Minimize Effect on Small Entities and Footnote #190 in the SEC Final Rule on Section 404.

TABLE 33. RELIANCE ON COSO 1992 COMPONENTS TO ASSESS INDUSTRY-SPECIFIC FRAUD RISK FACTORS

Five Components of the COSO 1992 Framework	Extent to which the SOX Compliance Team in your organization specifically relied upon the guidance provided by the five COSO 1992 components in assessing antifraud controls for industry-specific risk factors (N=239)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. Control Environment	9% (21)	26% (61)	23% (55)	29% (69)	14% (33)
2. Risk Assessment	9% (22)	28% (67)	26% (63)	22% (53)	14% (34)
3. Control Activities	9% (22)	28% (68)	24% (57)	25% (59)	14% (33)
4. Information and Communication	10% (25)	33% (78)	22% (53)	20% (48)	15% (35)
5. Monitoring	10% (25)	30% (72)	25% (60)	20% (47)	15% (35)

Note: Percentages are rounded.

TABLE 34. RELIANCE ON COSO 1992 COMPONENTS TO ASSESS MACRO-LEVEL FRAUD RISK FACTORS (OTHER THAN INDUSTRY-SPECIFIC RISK FACTORS)

Five Components of the COSO 1992 Framework	Extent to which the SOX Compliance Team in your organization specifically relied upon the guidance provided by the five COSO 1992 components in assessing macro-level antifraud risk factors (N=224)				
	No Extent	Some Extent	Moderate Extent	Large Extent	Uncertain
1. Control Environment	9% (21)	23% (52)	28% (63)	30% (67)	9% (21)
2. Risk Assessment	11% (25)	28% (62)	26% (59)	25% (55)	10% (23)
3. Control Activities	12% (27)	29% (65)	25% (56)	25% (55)	9% (21)
4. Information and Communication	13% (30)	31% (69)	26% (58)	20% (44)	10% (23)
5. Monitoring	13% (29)	26% (58)	29% (65)	22% (50)	10% (22)

Note: Percentages are rounded.

control over financial reporting are not omitted." In other words, if COSO 1992 is deemed to provide all the necessary guidance, why are the companies not using it to conduct their fraud risk assessments? Overall, the results presented in Tables 31–34 are worrisome because one of the major reasons for passing the SOX legislation was to put increasing focus on the assessment of potential fraud risk factors both by the company managements and their external auditors. It would be unfortunate if this critical goal of SOX was not achieved due to insufficiency of the guidance provided in COSO 1992 or the lack of skill set in companies and external auditors in applying the COSO 1992 guidance.

Provided below are the written comments made by our survey respondents as they relate to the discussion:

- We primarily relied on the publications offered by external accounting firms.
- Our mandatory antifraud assessment has all the characteristics of a tick-in-the-box approach. In our process documentation cycle, safeguarding of assets received sufficient attention to make a separate antifraud exercise of little added value.
- 1. AS2 is mandatory for the external auditors only. 2. Fraud risk is only within scope as it relates to risk of material error. 3. COSO is OK, but we built on it.
- Used practice aid showing antifraud programs and controls and white papers. Nothing from COSO.
- Guidance from the Big 4 public accounting firms (particularly PwC and Deloitte) was most helpful in this area.
- We primarily relied on the publications offered by external accounting firms.
- We used PwC's antifraud white paper as a benchmark for our companies' activities and a fraud risk assessment questionnaire provided by a Big 4 firm.
- We look at the controls that could possibly prevent fraud. However, in my experience, 90% of fraud was detected through someone reporting it. Otherwise, pretty much stumbled upon it.
- Macro-level antifraud controls applied were company-level controls related to our annual ethics compliance process as well as at the detailed control activity level relating to two items: (1) focus on identifying key control activities that address the financial statement assertion of validity to provide reasonable assurance that only valid transactions are processed; and (2) evaluation of segregation of duties during management's design effectiveness reviews.

V.2.C.3.c. Assessing IT Controls Using COSO 1992

The importance of assessing the effectiveness of general IT controls that support reliable financial disclosures is emphasized repeatedly in the guidance issued by the SEC and PCAOB.[96] General IT controls relate to: (1) Information technology control environment, (2) Program development, (3) Program change, (4) Access to programs and data, and (5) Computer operations.

These general IT controls apply to all IT systems, including spreadsheet applications, that provide information for the 10K and 10Q reports. Controls at third-party service providers that provide services that could impact on the company's external disclosures must also be assessed. Examples of these service providers include offshore software development firms, pension fund administrators, payroll services,

96 For example, see AS2 paragraphs 40, 50, 53, 73, and 75.

TABLE 35. FRAMEWORKS USED TO ASSESS EFFECTIVENESS OF INTERNAL CONTROLS OVER IT

Type of Control Model	# of Responses (N=373)	% of Total Responses
1. CobiT	193	51.7%
2. ITGI-A subset of the CobiT	36	9.7%
3. COSO 1992	165	44.2%
4. COSO ERM	7	1.9%
5. ISO 17779	14	3.8%
6. Uncertain	72	19.3%

software application service providers (ASPs), outsourced procurement, HR activities, and many others. These organizations may or may not be retaining outside experts to do SAS 70 Type II or local equivalent internal control reviews (e.g., CICA section 5900 is an example of the Canadian equivalent of a SAS 70 review) to assess and report on the existence and effectiveness of general IT controls and relevant application controls. In some cases, because general IT controls are so critical to the reliability of a company's external disclosures, the SAS 70 reviews that are currently being done at third-party sites may not be adequate to meet the SOX 302/404 expectations of external auditors.

Guidance provided by the SEC and PCAOB both indicate that it is important to recognize that companies must cover general IT controls that impact on the integrity of the general ledger and accounting systems and systems that store information used to prepare notes to the financial statements required by GAAP and in supplemental disclosures. This includes information stored in spreadsheet applications such as MS Excel.

The best guidance currently available to companies to complete general IT control reviews is ISO 17799 *Information Technology—Code of Practice for Information Security Management* and *IT Governance Institute IT Control Objectives for Sarbanes-Oxley*. Companies should first identify the full universe of the IT systems, including those controlled by service providers and internal spreadsheet applications that require assessment, and then assign responsibility for creating and maintaining these assessments. In addition to assessing general IT controls, companies must also consider IT-related risks that impact on all individual financial account and note disclosures.

To understand the use and relevance of COSO 1992 and the guidance provided by its five components to the evaluation and assessment

of IT controls, we asked a series of questions to our respondents. The first question in this series was "when assessing the effectiveness of your internal controls over IT to comply with SOX 404 requirements, which framework or standard did your organization use?" The answers are presented in Table 35. Note that percentages do not add to 100% for this question because we were interested in learning about all the frameworks that survey respondents used in assessing the effectiveness of IT controls in their companies.

The results presented in Table 35 indicate that the *CobiT—Control Objectives for Information and Related Technology Framework* issued by the IT Governance Institute was most often cited (approximately 52% of the time) by the survey respondents, followed by COSO 1992 (approximately 44% of the time). It is important to note that almost 20% of the respondents were uncertain about the framework their company used to assess and evaluate effectiveness of IT controls over financial reporting. When we analyze the sample responses by company size, we find that the pecking order displayed in Table 35 flips for small companies as they cite use of the COSO 1992 Framework more than the use of the CobiT Framework (56% vs. 41%).

The written responses provided by the survey participants are reproduced below:

- Focused on the 27 areas of CobiT that are directly linked to COSO framework.
- We created our own subset of CobiT objectives relevant for financial reporting, which largely coincides with ITGI-A subset.
- We are still remediating IT and are using the CobiT framework to do so.
- CobiT is the primary framework we are using. Our external auditors have given us tools to go from CobiT to COSO.
- We used CobiT and COSO last year to assure that we achieved adequate coverage for SOX 404 compliance. With the now more detailed PCAOB guidance in PCAOB 2 and Q&As we have switched to ITGI guidance.
- Followed Big 4 audit methodology, which pursues four domains—Security; Program Changes; Operations; Development and Implementation. CobiT in my view is way too detailed and overkill.
- CobiT was used for reference/guidance—not strict adherence.
- When it comes to IT, they tend to do things on their own. Their work must be integrated a lot more than it has. IT tends to keep things to themselves.

We further explored the survey participants on the assessment and evaluation of IT Governance and General IT Controls vs. IT Application Controls and their reliance on five COSO components to accomplish this task. Almost 95% of the respondents in our sample reported that their companies evaluated IT Governance and General IT Controls as well as IT application controls. Table 36 presents the answers to the following question:

- When evaluating IT Governance and General IT Controls, to what extent did your SOX compliance team specifically rely on the guidance provided by the COSO 1992 Framework for each one of the five COSO components of internal control? If you believe a certain COSO element does not apply to the IT Governance and General IT Controls, please choose not applicable.

The results indicate that only 17% to 25% of the respondents believe that their SOX compliance teams relied, to a large extent, on the guidance provided by the five COSO 1992 com-

TABLE 36. USE OF FIVE COSO 1992 COMPONENTS TO EVALUATE IT GOVERNANCE AND GENERAL IT CONTROLS

Five Components of the COSO 1992 Framework	Extent to which the SOX Compliance Team in your organization specifically relied upon the guidance provided by the five COSO 1992 components in assessing IT governance and general IT controls (N=305)					
	No Extent	Some Extent	Moderate Extent	Large Extent	COSO Element Does Not Apply	Uncertain
1. Control Environment	10% (31)	29% (89)	25% (76)	21% (63)	1% (4)	14% (42)
2. Risk Assessment	12% (38)	29% (89)	24% (74)	17% (52)	2% (5)	15% (47)
3. Control Activities	11% (35)	23% (69)	23% (69)	25% (77)	4% (11)	14% (44)
4. Information and Communications	12% (38)	29% (87)	23% (69)	18% (54)	2% (7)	16% (50)
5. Monitoring	13% (39)	27% (82)	25% (77)	18% (55)	3% (8)	14% (44)

Note: Percentages are rounded.

ponents. It is also important to note that a significant number (from 34% to 41%) believe that their SOX compliance teams relied on the COSO 1992 guidance either to no extent or only to some extent while evaluating their company's IT Governance and General IT controls. Similarly noteworthy is the finding that, on average, about 15% of the respondents are uncertain whether their SOX compliance teams relied on the COSO 1992 while evaluating IT controls. Almost the same results are repeated (see Table 37) when we ask the same question in respect to IT application controls.

Overall, it appears that the SOX compliance teams for our sample companies are relying on COSO 1992 only to a limited extent when it comes to assessing and evaluating IT controls over effective financial reporting. The written comments provided by the survey participants in response to this question are reproduced below:

- Our parent company provided internal audit staff that used COSO as their reference to technically evaluate our company's internal controls and communicated criteria to us. I simply disseminated their criteria to our company's IT and control process owners to carry out SOX compliance. I did not question the audit staff's interpretation of COSO 1992 Framework, nor did I read it for myself. Therefore, I am not familiar with this reference myself even though I know it was used as the basis for evaluating our internal controls.
- Both the control activities and information and communication components were relied upon heavily within the IT GCC control design.

TABLE 37. USE OF FIVE COSO 1992 COMPONENTS TO EVALUATE IT APPLICATION CONTROLS

Five Components of the COSO 1992 Framework	Extent to which the SOX Compliance Team in your organization specifically relied upon the guidance provided by the five COSO 1992 components in assessing IT application controls (N=300)					
	No Extent	Some Extent	Moderate Extent	Large Extent	COSO Element Does Not Apply	Uncertain
1. Control Environment	12% (37)	31% (93)	21% (64)	19% (57)	5% (14)	12% (35)
2. Risk Assessment	12% (36)	32% (97)	21% (64)	18% (54)	4% (12)	12% (37)
3. Control Activities	11% (33)	25% (74)	24% (72)	26% (79)	3% (8)	11% (34)
4. Information and Communications	14% (42)	33% (98)	22% (67)	14% (43)	3% (9)	14% (41)
5. Monitoring	13% (40)	30% (91)	22% (66)	18% (55)	4% (11)	12% (37)

Note: Percentages are rounded.

Key to the IT GCCs and the automated business-side control design is the communication of relevant information from systems during key detective reviews and to flag exceptions to automated control activities.

- The question I ask you is why do you assume that these should be in scope for SOX 404? Do a top-down, risk-based approach to find out; don't go bottom-up assuming you need these.
- Big 4 methodology and practice aids were used. Not COSO.
- COSO was not used. Separation of duties was obligatory considered in each process. Reports are identified based on key controls. Other application controls (interfaces, calculations) identified as required, but generally avoided.

V.2.C.3.D. Mapping Control Deficiencies to COSO 1992

As discussed earlier, AS2 states that the management is required to base its assessment of the effectiveness of internal control over financial reporting on a suitable control evaluation framework and that in the U.S., COSO 1992 meets the PCAOB's and SEC's criteria of a suitable framework. External auditors have, rightfully, interpreted this guidance to mean that "as part of management's Section 404 assessment, it must document, test, and evaluate the five components of the [COSO] internal control model."[97] Thus, it would seem to be a logical step for a company to map its discovered control deficiencies to the COSO criteria. Mapping

97 *Sarbanes-Oxley Act Section 404: Practical Guidance for Management*. PricewaterhouseCoopers, July 2004, p. 26.

TABLE 38. IS IT NECESSARY TO MAP CONTROL WEAKNESSES TO THE FIVE COSO 1992 COMPONENTS?

Response Statement	# of Responses (N=312)	% of Total Responses
1. No, it is not essential to map all discovered control deficiencies to COSO components to make such a claim.	99	31.7%
2. As long as an entity can demonstrate that it actively evaluated all five COSO components at the entity level, it is reasonable and sufficient to make such a claim.	150	48.1%
3. Yes, it is absolutely essential to clearly map all discovered control deficiencies to relevant COSO components to make such a claim.	40	12.8%
4. Uncertain	23	7.4%

of the discovered control weaknesses to each one of the five COSO 1992 components would help an evaluator understand the extent to which there are holes in each one of the five COSO 1992 components and whether the holes are so serious that a negative opinion on companies controls is warranted. Our pre-survey interviews confirm this thinking, as one of the Big 4 public accounting firms asks its clients to aggregate discovered control deficiencies, among other criteria, by five COSO categories to determine whether any one of these five categories has a material weakness in aggregation and is, therefore, rendered ineffective. Thus, mapping of the discovered control deficiencies would help a company evaluate whether each COSO component is sufficiently effective so as not to render the overall effectiveness claim "in accordance with COSO 1992 Framework" invalid. In the absence of such a mapping, we believe that a registrant will have a difficult time, if challenged by the regulatory authorities or in a lawsuit, to demonstrate that they actually evaluated their internal control over financial reporting in conformance to COSO 1992.

To understand the lack of disclosure in this area, we asked a series of three questions to our respondents. The first question is reproduced below:

- In your opinion, is it necessary to map all discovered control deficiencies to one or more of the five COSO components to claim that your company conducted its internal control assessment in accordance with the COSO 1992 Framework?

The results, presented in Table 38, provide interesting insights into how registrants are interpreting the relationship of discovered control weaknesses to the phrase "internal control evaluation conducted in accordance with *Internal Control—Integrated Framework*" [i.e., COSO 1992]. Only 13% of the respondents believe that it is absolutely essential to clearly map all discovered control deficiencies to relevant COSO components to legitimately claim that their internal control assessment was con-

TABLE 39. HOW MANY DID THE MAPPING?

Response Statement	# of Responses (N=312)	% of Total Responses
1. No, we did not map any of the discovered control deficiencies to any one of the COSO components.	105	33.7%
2. Yes, we only mapped some of the discovered control deficiencies to all the applicable COSO components.	42	13.5%
3. Yes, we clearly mapped all of the discovered control deficiencies to all the applicable COSO components.	73	23.4%
4. We did not need to map the discovered control deficiencies to the five COSO components because during the documentation process we had already mapped all of the controls to applicable COSO components.	65	20.8%
5. Uncertain	27	8.7%

ducted in accordance with COSO 1992 (see response #3). A staggering 32% of the respondents believe that it is not even necessary to do any such mapping to make the claim that their internal control assessment was done in accordance with COSO 1992 (See response #1). About 48% of the respondents take a middle-of-the-road position by stating that as long as a company can demonstrate that it evaluated at the entity-level (whatever that means) all five COSO components, it is sufficient and reasonable to make a claim in their SEC filings that their internal control assessment was done in accordance with COSO's *Internal Control—Integrated Framework*.

We further explored this topic by asking our respondents the following question regarding whether their SOX compliance teams did any such mapping:

- Did your SOX compliance team map all of the discovered control deficiencies to one or more of the five COSO components as part of the process of forming an opinion on the effectiveness of your organization's internal controls?

The results are presented in Table 39. Almost 34% of the respondents reported that their SOX compliance teams did not map the discovered control weaknesses to any of the five COSO components. Leaving out the 9% who were uncertain about such a mapping, we find that, of the remaining 58%, about 14% mapped only some of the discovered control deficiencies to one or more COSO components, about 24% clearly carried out this mapping, and about 21% proactively mapped all the controls (key or non-key) upfront to various COSO components during the documentation phase. This way, if a cer-

TABLE 40. HOW USEFUL IS COSO 1992 GUIDANCE IN MAPPING DISCOVERED CONTROL DEFICIENCIES?

Response Scale	# of Responses (N=178)	% of Total Responses
1. No Extent	16	9.0%
2. Some Extent	99	55.6%
3. Moderate Extent	39	21.9%
4. Large Extent	18	10.1%
5. Uncertain	6	3.4%

tain control was found to be inoperative either by design or in operation, the SOX compliance team members would already know which COSO components were impacted.

Since mapping of the discovered control weaknesses adds an extra step and additional costs to the SOX 404 compliance process, it would be important to understand the diversity of practice in this area and the basis of conclusion of those companies that claim to have done their control assessments in accordance with COSO's *Internal Control—Integrated Framework* so that others can also learn from their experiences. The last question in this series was asked to understand the usefulness of the guidance provided in COSO 1992 in helping companies map the discovered control deficiencies to one or more of the five COSO components. These results are presented in Table 40.

Only 10% of the respondents indicated that the guidance provided in COSO 1992 was useful to them to a large extent in mapping their control weaknesses to relevant COSO components.

About 65% of the respondents believed that the guidance provided by COSO 1992 was useful either to no extent or only to some extent when it came to aggregating the discovered control deficiencies by specific COSO components.

As part of our continuing research into various aspects of the control deficiency reporting, we have attempted to classify the publicly reported material control weaknesses into five COSO components. Our conclusion is that in some cases such a mapping cannot be done at least based on the information provided in the public disclosures. Our research also reveals that a large majority of the registrants are not disclosing their material control weaknesses by five COSO components.

V.2.D. Skills to Cost-Effectively Comply with SOX Requirements

Although it was the Cohen Commission Report in 1978 that called for management ownership of internal controls, experience indicates that, until the passage of SOX, internal audit was the dominant group involved in documenting, assessing, and reporting on an entity's system of internal

control. Due to the shortage of staff, rush for quarterly filings, staying on top of ever-increasing and complicated GAAP pronouncements, the role of the finance and controllership staff in this important activity was often very limited.

Similarly, due to fee pressures and the desire to cross-sell consulting services, external auditors treated financial audit as a loss leader. Compliance testing of internal controls was often eliminated in total or to a large extent by setting the control risk to 100%. Audit opinions were being issued solely based on the results of limited substantive testing and analytical procedures. As a result of this trend, risk and control assessment and reporting received little or no attention in the professional training programs and business school curricula.[98] Consequently, a large number of today's CEOs and CFOs appear to have received very little training in conducting formal risk and control assessments. As a matter of fact, a large majority of these managers have a very negative opinion of internal control and associate it with something that constrains their decision making and the organization's entrepreneurial spirit.

We believe that lack of adequate skills and proper training in risk and control assessments is another significant factor that is contributing to the current levels of frustrations and massive implementation costs. To explore issues related to the skill-set or training, we asked our respondents for their views on the skills and knowledge relevant for cost-effective compliance with SOX 302/404.

We start this discussion by first assessing the level of individual competence that our survey respondents believe they have in applying COSO 1992. Table 41 presents these responses.

Only 24% of the survey participants feel that they are experts in applying COSO 1992 as it relates to conducting internal control assessment pursuant to Sections 302/404. About 59% claim that they are not experts in applying the COSO 1992 Framework but believe that they can make it work to help their companies comply with the internal control requirements under SOX. Although these results do not change significantly when we analyze the sample by company size and job title, the information provided in Table 42 sheds some additional light on the lack of competency that our survey respondents feel in applying COSO 1992 to meet SOX requirements.

From Table 42 we find that, as expected, internal auditors generally are more comfortable in applying the COSO 1992 guidance than the management-types in our sample. Only 20% of the respondents from smaller public companies vs. 25% from medium-to-large public companies feel that they are experts in applying COSO 1992.

Next, we focused on assessing the relative importance of various skills and competencies for cost-effective SOX 302/404 compliance. This skill inventory is reproduced below and

98 In the pre-SOX era, the internal control-related discussions were held in the external or internal auditing-related courses only. Nonaccounting majors typically graduated with no exposure to the concepts of risk and control. Unfortunately, even four years after the passage of the Sarbanes-Oxley Act, the business schools have not caught up with the idea that risk and control-related training is an absolute must for all business school graduates because many of them will grow up to be CEOs and CFOs and will be signing on the dotted-line that they take personal responsibility about the effectiveness of internal controls in their organizations without ever having to take a single course in risk and control.

TABLE 41. LEVEL OF INDIVIDUAL COMPETENCY IN APPLYING COSO 1992 GUIDANCE

Level of Competency	# of Responses (N=283)	% of Total Responses
1. I am an expert in applying the COSO 1992 Framework in my company.	67	23.7%
2. I am not an expert in applying the COSO 1992 Framework but I can make it work.	166	58.7%
3. I am somewhat unfamiliar with how to really apply the COSO 1992 Framework.	34	12.0%
4. I really struggle with applying the COSO 1992 Framework.	3	1.1%
5. I'm uncertain about my level of competency in applying COSO 1992.	13	4.6%

TABLE 42. LEVEL OF INDIVIDUAL COMPETENCY IN APPLYING COSO 1992 GUIDANCE BY COMPANY SIZE AND JOB TITLE

Level of Competence	Company Size		Job Title	
	Small Company (N=54)	Medium to Large Company (N=229)	Internal Auditor Responses (N=126)	Management-type Responses (N=157)
1. I am an expert in applying the COSO 1992 Framework in my company.	20.4% (11)	24.5% (56)	28.6% (36)	19.7% (31)
2. I am not an expert in applying the COSO 1992 Framework but I can make it work.	61.1% (33)	58.1% (133)	59.5% (75)	58.0% (91)
3. I am somewhat unfamiliar with how to really apply the COSO 1992 Framework.	14.8% (8)	11.4% (26)	8.7% (11)	14.6% (23)
4. I really struggle with applying the COSO 1992 Framework.	0.0% (0)	1.3% (3)	0.8% (1)	1.3% (2)
5. I'm uncertain about my level of competency in applying COSO 1992.	3.7% (2)	4.85% (11)	2.4% (3)	6.4% (10)

was generated as a result of our pre-survey fieldwork and interviews:

1. Ability to understand and apply existing risk models.
2. Ability to understand and apply current control models (such as COSO 1992, COSO ERM, etc.) that are the dominant models for SOX 404 reporting.
3. Ability to understand and apply the control model that a CEO/CFO uses to report against under Section 302 of SOX.
4. Ability to reasonably assess the residual risk status associated with various financial statement accounts and note disclosures.
5. Ability to determine in a most efficient manner the key controls in a business organization.
6. Ability to create relevant process flowcharts and narratives with needed information.
7. Ability to determine how much internal control testing is necessary to conclude whether a company has an effective system of internal control over financial reporting.
8. Ability to correctly identify underlying internal control weaknesses by examining discovered control exceptions.
9. Ability to correctly grade discovered internal control deficiencies as a significant control deficiency or a material control weakness per AS2.
10. Ability to evaluate the discovered control deficiencies by identifying the relevant aggregation criteria per AS2.
11. Ability to understand and apply numerous other requirements of AS2 to ensure that a registrant is in compliance with SOX 302/404.
12. Ability to independently conduct a risk and control self-assessment.
13. Ability to evaluate the reliability of self-assessment information produced by process/account owners.
14. Ability to determine the cost vs. benefit of obtaining additional assurance on a registrant's system of internal control over financial reporting.
15. Ability to use the skills learned through SOX to competently identify and assess the risks and controls in other areas such as safety, regulatory compliance, product quality, cost control, etc.

We converted the above mentioned skill-set inventory into a series of three questions to understand the extent to which our survey respondents believe each skill is important to learn by various members of the (1) SOX compliance implementation team, (2) external audit team, and (3) consultants assisting on SOX related projects. Tables 43-45 summarize these results.

The results presented in Table 43 indicate that an overwhelming number of survey respondents believe that the following three skills are absolutely essential for SOX compliance team members to cost-effectively comply with SOX 302/404 requirements:

1. Skill #5: Ability to determine in a most efficient manner the key controls in a business organization. (81%)
2. Skill #7: Ability to determine how much internal control testing is necessary to conclude whether a company has an effective system of internal control over financial reporting. (74%)
3. Skill #8: Ability to correctly identify underlying internal control weaknesses by examining discovered control exceptions. (79%)

The highest ranking accorded to these three skills is noteworthy. First, a significant amount of current debate on what is driving the high

TABLE 43. SKILLS NEEDED FOR THE SOX IMPLEMENTATION TEAM MEMBERS

Type of Skill	No Extent to Some Extent	(N=283) Moderate Extent	Large Extent to Absolutely Essential
1. Being able to understand and apply existing risk models.	14% (39)	28% (79)	58% (165)
2. Being able to understand and apply current control models (such as COSO 1992, COSO ERM, etc.) that are the dominant models for SOX 404 reporting.	14% (39)	34% (96)	52% (148)
3. Being able to understand and apply the control model that my CEO/CFO uses to report against under Section 302 of SOX.	20% (58)	31% (87)	49% (138)
4. Being able to reasonably assess the residual risk status associated with various financial statement accounts and note disclosures.	16% (47)	37% (106)	46% (130)
5. Being able to determine in a most efficient manner the key controls in my organization.	6% (17)	13% (37)	81% (229)
6. Being able to create relevant process flowcharts and narratives with needed information.	18% (50)	35% (99)	47% (134)
7. Being able to determine how much internal control testing is necessary to conclude whether we have an effective system of internal control over financial reporting.	5% (15)	21% (60)	74% (208)
8. Being able to correctly identify underlying internal control weaknesses by examining discovered control exceptions.	4% (11)	17% (47)	79% (225)
9. Being able to correctly grade discovered internal control deficiencies as a significant control deficiency or a material control weakness.	7% (20)	25% (70)	68% (193)
10. Being able to evaluate the discovered control deficiencies by identifying the relevant aggregation criteria.	11% (32)	35% (100)	53% (151)
11. Being able to understand and apply numerous other requirements of AS2 to ensure that my company is in compliance with SOX 302/404.	15% (43)	33% (93)	52% (147)
12. Being able to independently conduct a risk and control self-assessement.	18% (51)	35% (98)	47% (134)
13. Being able to evaluate the reliability of self-assessment information produced by process/account owners.	22% (61)	30% (85)	48% (137)
14. Being able to determine the cost vs. benefit of obtaining additional assurance on my company's system of internal control over financial reporting.	25% (71)	34% (95)	42% (117)
15. Being able to use the skills learned through SOX to competently identify and assess the risks and controls in other areas, such as safety, regulatory compliance, product quality, cost control, etc.	32% (92)	29% (83)	38% (108)

Note: Percentages are rounded.

SOX compliance costs has centered around the difficulty experienced by SOX compliance team members in determining *what is* and *what is not* a key control. Registrants have told horror stories to the SEC commissioners about thousands of key controls being identified by their external auditors for potential testing and assessment. Second, registrant personnel have experienced a great deal of difficulty in ascertaining whether a discovered control exception is a one-time event or an underlying control weakness. This is because most of the publicly reported internal control weaknesses were discovered, at least during year one of complying with SOX 302/404, by the external auditors during the process of conducting the financial audit. In such a case, the registrants had no choice except to admit that there is some deficiency in their internal controls over financial reporting. Having admitted the deficiency, now it became incumbent upon management to assign the discovered control deficiency to some internal control weakness for public reporting purposes. Third, the issue of when enough is enough to conclude whether a company has an effective internal control system over its financial reporting has also been thought of as a major cost driver to high costs of SOX compliance.

Table 44 evaluates the same skill-set but this time for an external auditor. The following three skills were considered absolutely essential by our survey respondents for an external auditor to have.

1. Skill #7: Ability to determine how much internal control testing is necessary to conclude whether a company has an effective system of internal control over financial reporting. (80%)
2. Skill #8: Ability to correctly identify underlying internal control weaknesses by examining discovered control exceptions. (77%)
3. Skill #9: Ability to correctly grade discovered internal control deficiencies as a significant control deficiency or a material control weakness per AS2. (79%)

It is noteworthy that skill #7, which deals with "determining how much testing is enough to conclude whether a company has an effective internal control system," and skill #8, which deals with the "ability to correctly identify underlying internal control weakness by examining the discovered control deficiency," again top the list as an important skill, this time for an external auditor to have in order to conduct a cost-effective SOX 302/404 assessment. Interestingly, our respondents believe that for an external auditor the skill of being able to correctly grade the discovered control deficiencies into the two buckets of significant control deficiency and a material control weakness (skill #9) is equally important. In hindsight, it makes sense because if an external auditor would incorrectly classify discovered control deficiencies, either individually or in aggregate, as a material control weakness, it may have serious repercussions for the registrant in the capital markets. Further, there is extensive evidence in the various feedbacks and comment letters filed with the SEC that the definitions of "more than remote" and "more than inconsequential" are not that easy to apply in practice.

It is no secret that a plethora of boutique consulting practices have emerged in the post-SOX era with the sole objective of helping companies compile extensive documentation and conduct testing of internal controls to pass their Section 404 certification by their external auditors. Thus, it is important to understand what skills the registrant personnel consider impor-

TABLE 44. SKILLS NEEDED FOR THE EXTERNAL AUDITORS

Type of Skill	No Extent to Some Extent	(N=283) Moderate Extent	Large Extent to Absolutely Essential
1. Being able to understand and apply existing risk models.	10% (27)	25% (72)	65% (184)
2. Being able to understand and apply current control models (such as COSO 1992, COSO ERM, etc.) that are the dominant models for SOX 404 reporting.	10% (30)	28% (79)	62% (174)
3. Being able to understand and apply the control model that my CEO/CFO uses to report against under Section 302 of SOX.	23% (65)	25% (70)	52% (148)
4. Being able to reasonably assess the residual risk status associated with various financial statement accounts and note disclosures.	9% (28)	22% (63)	66% (192)
5. Being able to determine in a most efficient manner the key controls in my organization.	12% (33)	16% (46)	62% (204)
6. Being able to create relevant process flowcharts and narratives with needed information.	38% (107)	32% (91)	30% (85)
7. Being able to determine how much internal control testing is necessary to conclude whether we have an effective system of internal control over financial reporting.	5% (13)	15% (43)	80% (227)
8. Being able to correctly identify underlying internal control weaknesses by examining discovered control exceptions.	4% (11)	18% (52)	77% (220)
9. Being able to correctly grade discovered internal control deficiencies as a significant control deficiency or a material control weakness.	4% (12)	17% (48)	79% (223)
10. Being able to evaluate the discovered control deficiencies by identifying the relevant aggregation criteria.	9% (27)	20% (58)	70% (198)
11. Being able to understand and apply numerous other requirements of AS2 to ensure that my company is in compliance with SOX 302/404.	9% (25)	20% (57)	71% (201)
12. Being able to independently conduct a risk and control self-assessement.	30% (85)	28% (78)	42% (120)
13. Being able to evaluate the reliability of self-assessment information produced by process/account owners.	22% (64)	27% (77)	50% (142)
14. Being able to determine the cost vs. benefit of obtaining additional assurance on my company's system of internal control over financial reporting.	25% (72)	28% (79)	47% (132)
15. Being able to use the skills learned through SOX to competently identify and assess the risks and controls in other areas, such as safety, regulatory compliance, product quality, cost control, etc.	43% (120)	26% (73)	31% (90)

Note: Percentages are rounded.

TABLE 45. SKILLS NEEDED FOR THE SOX CONSULTANTS

Type of Skill	No Extent to Some Extent	(N=283) Moderate Extent	Large Extent to Absolutely Essential
1. Being able to understand and apply existing risk models.	10% (28)	20% (57)	70% (198)
2. Being able to understand and apply current control models (such as COSO 1992, COSO ERM, etc.) that are the dominant models for SOX 404 reporting.	11% (31)	19% (55)	70% (197)
3. Being able to understand and apply the control model that my CEO/CFO uses to report against under Section 302 of SOX.	18% (51)	20% (58)	62% (174)
4. Being able to reasonably assess the residual risk status associated with various financial statement accounts and note disclosures.	13% (35)	20% (58)	77% (190)
5. Being able to determine in a most efficient manner the key controls in my organization.	8% (21)	13% (37)	79% (225)
6. Being able to create relevant process flowcharts and narratives with needed information.	15% (40)	21% (60)	65% (183)
7. Being able to determine how much internal control testing is necessary to conclude whether we have an effective system of internal control over financial reporting.	10% (26)	14% (39)	77% (218)
8. Being able to correctly identify underlying internal control weaknesses by examining discovered control exceptions.	10% (28)	19% (55)	70% (200)
9. Being able to correctly grade discovered internal control deficiencies as a significant control deficiency or a material control weakness.	12% (33)	24% (67)	64% (183)
10. Being able to evaluate the discovered control deficiencies by identifying the relevant aggregation criteria.	13% (38)	27% (77)	69% (168)
11. Being able to understand and apply numerous other requirements of AS2 to ensure that my company is in compliance with SOX 302/404.	13% (38)	19% (53)	77% (192)
12. Being able to independently conduct a risk and control self-assessement.	20% (59)	19% (54)	60% (170)
13. Being able to evaluate the reliability of self-assessment information produced by process/account owners.	20% (57)	22% (63)	67% (163)
14. Being able to determine the cost vs. benefit of obtaining additional assurance on my company's system of internal control over financial reporting.	18% (51)	22% (61)	61% (171)
15. Being able to use the skills learned through SOX to competently identify and assess the risks and controls in other areas, such as safety, regulatory compliance, product quality, cost control, etc.	32% (91)	23% (64)	45% (128)

Note: Percentages are rounded.

tant for such consultants. Table 45 presents the results of the ranking of the same skill-set inventory but with respect to the SOX consultants.

From a review of the results presented in Table 45, the following four skills are considered important for the SOX consultants to have:

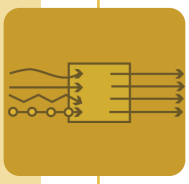
1. Skill #4: Being able to reasonably assess the residual risk status associated with various financial statement accounts and note disclosures. (77%)
2. Skill #5: Ability to determine in a most efficient manner the key controls in a business organization. (79%)
3. Skill #7: Ability to determine how much internal control testing is necessary to conclude whether a company has an effective system of internal control over financial reporting. (77%)
4. Skill #11: Ability to understand and apply numerous other requirements of AS2 to ensure that a registrant is in compliance with SOX 302/404. (77%)

Once again, skill #7 reappears and is considered very important for a SOX consultant to have. However, the survey respondents believe that skills #4, #5, and #11 are also important for a SOX consultant to effectively help a client in meeting requirements of the Section 404 certification. What is interesting here is that for the first time the skill of assessing the residual risk status makes the list. It is not at all clear to us as why our respondents consider this skill to be an important one for the consultant to posses but not for the SOX compliance team members or company's external auditors.

Although for discussion purposes we chose to highlight only the top three to four skills for each position, it would not be incorrect to conclude that most of the respondents believe that a significant majority of the 15 skills presented by us in Tables 43–45 are important for all the parties involved in the SOX compliance process.

VI. EPILOGUE

The Sarbanes-Oxley Act of 2002 is a landmark piece of legislation that clearly thrusts control governance to the forefront and squarely puts the responsibility for effective internal controls over financial reporting where it truly belongs: the company management. As early as 1776, Adam Smith, father of modern-day capitalism, in his famous treatise, *Inquiry into the Nature and Causes of the Wealth of Nations,* wrote, "…being the managers of other people's money rather than their own, it cannot well be expected that [managers] should watch over it with the same anxious vigilance with which [they would watch over their own money]." Holding management responsible and accountable for maintaining effective internal controls over financial reporting, to a large extent, would mitigate the inherent conflict, as identified by Adam Smith, that exists among the suppliers and the providers of capital in a free market system. Additionally, per the requirements of Section 302 and 404 holding management accountable for maintaining an effective internal control system that produces financial disclosures along with faithfully communicating all discovered material weaknesses in this system to their external auditors considerably enhances the quality of an auditors' attestation opinion. Armed with the knowledge about the true state of effectiveness of a company's internal controls over financial reporting, the auditor can now determine the scope of the attestation engagement as well as design and choose appropriate substantive audit tests to opine on the fairness of financial disclosures of a client.



In theory, all of this makes perfect sense. The fact that many other industrialized countries and regions with equally developed and sophisticated capital markets (i.e., Canada, United Kingdom, European Union, Australia, etc.) have considered and consciously made a decision not to go the route of Section 404 internal control certifications confirms that a large majority of these countries believe that the U.S. has not yet gotten the management reporting of internal control over financial reporting right. The SEC Chairman, Christopher Cox, while concluding his opening remarks to the SEC/PCAOB-sponsored *Roundtable on Second-Year Experiences with Internal Control Reporting Requirements* noted, "I hope and expect that today's Roundtable will bring us much closer to the finish line. We have every intention at the SEC and at the PCAOB to get 404 right sooner rather than later."

Consistent with Chairman Cox's remarks referring to AS2 that "no similar guide, however, exists for companies and for their management," one can surmise that a control framework for management assessment and reporting on internal control is the pivotal element in ensuring cost-effective compliance with SOX 302/404. This research study highlights the fact that SOX implementation teams across the companies represented in our sample are not overwhelmingly utilizing the guidance provided by the COSO 1992 Control Framework to base their internal control assessments. The primary reason for this nonreliance is the principles-based nature of the COSO 1992 Framework that lacks management-centric and risk-based implementation guidance from the perspective of management. Thus, in response to Chairman Cox's question, "Wouldn't management benefit from having guidance from the Securities and Exchange Commission on what constitutes adequate controls?" this research study's findings suggest that maybe the time has come for regulatory agencies and standard-setters to reconsider the suitability of the COSO 1992 Framework for use by the registrants to assess the effectiveness of their internal controls over financial reporting.

USEFUL LINKS

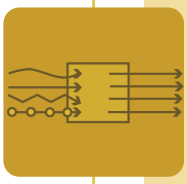
1. Sarbanes-Oxley Act of 2002, House of Representatives 3763. http://www.loc.gov/law/guide/pl107204.pdf

2. SEC Final Rule on Section 302: Certification of Disclosure in Companies' Quarterly and Annual Reports. http://www.sec.gov/rules/final/33-8124.htm

3. SEC Final Rule on Section 404: Management's Reports on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. http://www.sec.gov/rules/final/33-8238.htm

4. PCAOB Release No. 2004-001: An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, Auditing Standard No. 2, March 9, 2004. http://www.pcaobus.org/Rules/Docket_008/2004-03-09_Release_2004-001-all.pdf

5. FASB Statement of Financial Accounting Standards No. 5: Accounting for Contingencies, March 1975. http://www.fasb.org/pdf/fas5.pdf



6. SEC Staff Accounting Bulletin No. 99: Materiality, August 12, 1999. http://www.sec.gov/interps/account/sab99.htm

7. SEC Division of Corporation Finance: Frequently Asked Questions—Management's Report on Internal Control over Financial Reporting and Disclosure in Exchange Act Periodic Reports. Revised October 6, 2004, Questions 1-23. http://www.sec.gov/info/accountants/controlfaq1004.htm

8. SEC Division of Corporation Finance Frequently Asked Questions Management's Report on Internal Control over Financial Reporting and Related Auditor Report, January 21, 2005. http://www.sec.gov/divisions/corpfin/faq012105.htm

9. SEC Division of Corporation Finance and the Office of the Chief Accountant: Staff Statement on Management's Report on Internal Control over Financial Reporting, May 16, 2005. http://www.sec.gov/info/accountants/stafficreporting.htm

10. PCAOB Staff Questions and Answers: Auditing Internal Control over Financial Reporting. Questions 1-26 issued on June 23, 2004. http://www.pcaobus.org/Standards/Staff_Questions_and_Answers/2004/06-23.pdf

    Questions 27-29 issued on October 6, 2004. http://www.pcaobus.org/Standards/Staff_Questions_and_Answers/2004/10-06.pdf

    Questions 30-36 issued on November 22, 2004. http://www.pcaobus.org/Standards/Staff_Questions_and_Answers/2004/11-22.pdf

    Question 37 issued on January 21, 2005. http://www.pcaobus.org/Standards/Staff_Questions_and_Answers/2005/01-21.pdf

    Questions 38-55 issued on May 16, 2005. http://www.pcaobus.org/Standards/Staff_Questions_and_Answers/2005/05-16.pdf

11. PCAOB Release No. 2005-009: Policy Statement Regarding Implementation of Auditing Standard No. 2: An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements, May 16, 2005. http://www.oversightsystems.com/pdfs/PCAOB_PolicyStatement05162005.pdf

12. Institute of Internal Auditors: Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control, June 10, 2005. http://www.theiia.org/download.cfm?file=25663

13. PricewaterhouseCoopers: Key Elements of Antifraud Programs, November 2003. http://www.pwc.com/Extweb/manissue.nsf/docid/23FDB9805FEE7EC085256CD20062978F

14. PricewaterhouseCoopers: The Use of Spreadsheets—Considerations for Section 404 of the Sarbanes-Oxley Act, July 2004. http://www.pwc.com/extweb/service.nsf/docid/CD287E403C0AEB7185256F08007F8CAA

15. Tim Leech and Parveen Gupta Comment Letter to SEC in Response to Request for Comments on Section 404, April 1, 2005. http://www.sec.gov/news/press/4-497/tjleech9545.pdf

16. SEC's Transcript of the May 10, 2006 Roundtable on Second-Year Experiences with Internal Control Reporting and Auditing Provisions. http://www.sec.gov/spotlight/soxcomp/soxcomp-transcript.txt

17. Briefing Paper: Roundtable on Second-Year Experiences with Internal Control Reporting and Auditing Provisions, May 1, 2006. http://www.sec.gov/spotlight/soxcomp/soxcomp-briefing0506.htm

18. SEC Announces Next steps for Sarbanes-Oxley Implementation, Press Release No. 2006-75, May 17, 2006. http://www.sec.gov/news/press/2006/2006-75.htm

19. SEC's Concept Release Concerning Management' Reports on Internal Control over Financial Reporting, July 11, 2006. http://www.sec.gov/rules/concept/2006/34-54122.pdf

LIST OF TABLES

INSTITUTE OF MANAGEMENT ACCOUNTANTS

Research Advisory and Review Board

Tim Leech, FCA-CIA, CCSA, CFE
Principal Consultant and Chief Methodology Officer
Paisley Consulting

Bruce McCuaig, CA-CIA, CCSA
Principal Consultant
Paisley Consulting

Sandra B. Richtermeyer, Ph.D., CMA, CPA
Associate Professor and IMA's Professor-in-Residence
Xavier University

Steven J. Root, CPA, CIA
Director of Finance, Administration, and Processes and
Chief Audit Executive (Retired)
Northrop Grumman

William G. Shenkir, Ph.D., CPA
William Stamps Farish Professor of Free Enterprise
McIntire School of Commerce
University of Virginia

Mark C. Southon
Director, Enterprise Risk Management
The PMI Group, Inc.

Patrick J. Stroh, CMA
Executive Director
United Health Group, Inc.

Jeffrey C. Thomson, M.S.
Vice President-Research and Applications Development
Institute of Management Accountants

Betsy Socci, CPA
Former Financial Reporting Specialist
OraSure Technologies, Inc.

Michael R. Zanoni, CPA
Director, Financial Compliance
Boeing Corporation

SURVEY INSTRUMENT

To: Each Respondent
From: Paul Sharman, President and CEO, Institute of Management Accountants or Dave Richards, President, Institute of Internal Auditors

The IMA is embarking on major initiatives to address a burning issue in business today: How to comply with Sarbanes-Oxley (SOX) Sections 302 and 404 while addressing practitioner concerns related to:

- Improving the quality of financial and operational reporting
- Lowering costs of SOX compliance
- Focusing on strategic and operational risks rather than only on financial controls
- Accelerating rather than delaying investments
- Building sustainable improvements in staff competencies and business processes

We are requesting your help to complete this survey. We consider your opinions very valuable. Please note that your responses to this survey will be relied upon to launch a number of policy initiatives going forward including development of an e-learning series on SOX, a more advanced curriculum on enterprise risk and controls leading to two specialized certificates, and the design of a practical and management-friendly assurance and assessment framework that will make it much less onerous for you to comply with SOX-like legislations. We also plan to utilize the survey results to develop

position papers that would propose practical changes to the SOX regulatory regime to ease the compliance burden on businesses while retaining the spirit of the corporate governance reforms put into place by SOX. Thus, this survey has two specific purposes: (1) to seek candid feedback on implementation related issues with the COSO control framework and (2) to identify any skill gaps that you may have encountered either in your SOX implementation staff, consultants or your external auditors while complying with Sections 302/404 of the Sarbanes-Oxley Act of 2002.

For each question, please choose the answer that best captures your opinion based on your SOX implementation experience. We encourage you to use the space provided below to express any views that were not captured adequately in your multiple choice response. Your responses to this survey will be confidential. We will only publish aggregated survey results in the form of a research study. We have retained Dr. Parveen P. Gupta, a professor of accounting, from Lehigh University to conduct this survey and prepare a research report for the IMA.

We realize that your time is valuable and your opinions are very important to us. Please complete the survey within one week. All respondents will receive a free copy of the research report based on the survey results and a priority invitation and registration in an IMA sponsored webcast in the first half of next year to review and discuss with other webcast participants the implications of the survey results for management decision making.

Please be candid and thorough in your responses as the issues discussed in this survey are of utmost importance to all of us.

SECTION I: DEMOGRAPHIC INFORMATION

1. Which of the following job titles best describe your current position?
   - O Chief Financial Officer
   - O Vice President
   - O Controller
   - O Assistant Controller
   - O SOX Implementation In-Charge/Specialist
   - O Accounting Manager or Supervisor
   - O External Auditor
   - O Internal Auditor
   - O Other (please specify)

2. Do you have any formal auditing and accounting certification (e.g. CMA, CPA, CIA, etc.?)
   - O Yes
   - O No
   - O If yes, please state

3. How many years of accounting and finance experience do you have?

	1 to 5	6 to 10	11 to 15	16 to 20	21+
Overall experience in all positions held in your career	O	O	O	O	O
Experience only in the current position	O	O	O	O	O

4. What is the primary industry in which your company operates?
   - O Education
   - O Healthcare
   - O Media and Entertainment
   - O Construction, Mining, Agriculture
   - O Manufacturing
   - O Transportation, Communication, Utilities
   - O Wholesale/Retail
   - O Financial Services
   - O Insurance
   - O Business Services
   - O Real Estate
   - O High Tech
   - O Pharmaceuticals & Biotechnology
   - O Government
   - O Non-profit
   - O Other (please specify)

5. What are the annual revenues of your company for the most recent fiscal year-end?

- O Under $1 million
- O More than $1 million but less than $10 million
- O More than $10 million but less than $100 million
- O More than $100 million but less than $500 million
- O More than $500 million but less than $1 billion
- O More than $1 billion but less than $5 billion
- O More than $5 billion but less than $10 billion
- O More than $10 billion
- O Do not wish to disclose
- O Not applicable

6. What are the total assets of your company as of the most recent fiscal year-end?

- O Under $50 million
- O More than $50 million but less than $100 million
- O More than $100 million but less than $250million
- O More than $250 million but less than $500 million
- O More than $500 million but less than $1 billion
- O More than $1 billion but less than $5 billion
- O More than $5 billion but less than $10 billion
- O More than $10 billion
- O Do not wish to disclose
- O Not applicable

7. How many employees are in your company?

- O Under 500
- O 501-1,000
- O 1,001-2,500
- O 2,501-5,000
- O 5,001-7,500
- O 7,501-10,000
- O 10,001-15,000
- O More than 15,001

8. What percentage of your time is spent managing or working on the projects related to the SOX 302/404 compliance?
   - O Less than 10%
   - O 11% – 20%
   - O 21% – 30%
   - O 31% – 40%
   - O 41% – 50%
   - O 51% – 75%
   - O More than 75%
   - O None

9. What is the current status of your company with respect to Sarbanes-Oxley compliance?
   - O Publicly traded company–Accelerated Filer
   - O Publicly traded Company–Non-Accelerated Filer
   - O Non-publicly traded company
   - O Foreign Private Issuer
   - O Not-for-profit organization
   - O Governmental organization
   - O Other (please state)

10. What is the current status of your company with respect to the SOX 302/404 certification?
    - O We have already filed our first annual internal control certification under SOX 404
    - O We are working towards filing our first annual internal control certification under SOX 404 in the near future
    - O Although our organization is not subject to the requirements of SOX 302/404 certification requirements, we are conducting internal control assessments under Sections 302/404 on a voluntary basis
    - O Since our organization is not subject to SOX 302/404 certification requirements for internal control assessments, we are not conducting such internal control assessments

END OF SECTION I

SECTION II: SOX 302/404 RELATED GENERAL QUESTIONS

Unless stated otherwise, please note that all of the questions that follow in this and all other sections of this survey relate to your first-year Section 302/404 certification experiences irrespective of whether you have already filed your first certification or you are in the process of preparing to file such a certification in the near future.

11. For each one of the following SOX compliance activities indicate by putting a check mark under the group or function that was primarily responsible for each activity in your organization. If a certain activity did not occur at your organization, please choose not applicable. You may choose more than one group for each activity.

SOX Compliance Activities	Not Applicable	Entity-level Compliance Group	Internal Auditing	Financial Reporting Function	Operations or Process Owners	IT Function
1. Creating Process Documentation	O	O	O	O	O	O
2. Maintaining Process Documentation	O	O	O	O	O	O
3. Identification of Risks	O	O	O	O	O	O
4. Identification of Related Controls	O	O	O	O	O	O
5. Testing of Key Controls	O	O	O	O	O	O
6. Self Assessment	O	O	O	O	O	O
7. Remediation of Exceptions	O	O	O	O	O	O
8. Coordinating the Audit with External Auditors	O	O	O	O	O	O

12. Indicate, by putting a check-mark, the extent to which each of the following SOX compliance related activities were costly to your organization. If a certain activity did not occur at your organization, please choose not applicable.

SOX Compliance Activities	Not costly at all	Not particularly costly	Somewhat costly	Very costly	Not applicable
1. Creating and Maintaining Process Documentation	O	O	O	O	O
2. Testing of Key Controls	O	O	O	O	O
3. Self-assessment by Process Owners	O	O	O	O	O
4. Remediation Related Activities	O	O	O	O	O
5. Attestation and Certification	O	O	O	O	O
6. Staff Training	O	O	O	O	O
7. Investment in New Tools and Technology	O	O	O	O	O

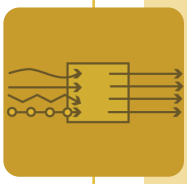
13. In your opinion, what percentage of the documentation and testing, whether done by your organization or its external auditors, was unnecessary to "reasonably" conclude that your organization has an effective system of internal control over financial reporting?
    - O Less than 10%
    - O 11% – 20%
    - O 21% – 30%
    - O 31% – 40%
    - O 41% – 50%
    - O 51% – 75%
    - O More than 75%
    - O None

14(a). Indicate, by putting a check mark, for each of the following SOX compliance related activities, whether your organization is experiencing an increase or decrease in its SOX compliance costs relative to year-one implementation efforts.

SOX Compliance Activities	Increase	Decrease	Not applicable
1. Creating and Maintaining Process Documentation	O	O	O
2. Testing of Key Controls	O	O	O
3. Self-assessment by Process Owners	O	O	O
4. Remediation Related Activities	O	O	O
5. Attestation and Certification	O	O	O
6. Staff Training	O	O	O
7. Investment in New Tools and Technology	O	O	O

14(b). If your organization has experienced an increase or decrease in its SOX compliance costs tell us how much going into the year-two certification effort.

SOX Compliance Activities	Increase—By how much? Drop down menu of choices: Less than 5% 5% to 10% 11% to 15% 16% to 20% More than 20% Not applicable	Decrease—By how much? Drop down menu of choices: Less than 5% 5% to 10% 11% to 15% 16% to 20% More than 20% Not applicable
Creating and Maintaining Process Documentation	O	O
Testing of Key Controls	O	O
Self-assessment by Process Owners	O	O
Remediation Related Activities	O	O
Attestation and Certification	O	O
Staff Training	O	O
Investment in New Tools and Technology	O	O



15. To what extent, you believe, your external auditors are conducting an integrated audit as defined by the PCAOB Auditing Standard No. 2 during your current year certification process?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Too early to tell

16. Did your organization take a "risk-based" approach to its SOX compliance efforts? (By "risk-based" approach we mean focusing on the acceptability of the "residual risk status" of those business processes that most likely will result in control deficiencies based on your historical error rates etc.) Please read all choices before answering the question.
    - O We took a risk based approach in the way it is described in the question.
    - O We took a top-down risk based approach to define the scope of our work but did not identify or focus on the "residual risk" the way it is described in the question.
    - O We implemented a bottom-up approach by first documenting all processes and identifying all of the internal controls in the process, and then testing them exhaustively to conclude whether we have an effective system of internal control over financial reporting to certify under Sections 302/404.
    - O We did focus on the risks but not in the way the question describes it. (In the space provided below, briefly describe your approach and how you focused on the risks.)
    - O Uncertain as to the approach that we took.

17. For the majority of your financial statement accounts to what extent did your SOX compliance team identify the plausible risks that could threaten the integrity of the balance in each one of the accounts?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain

18. For the majority of your financial statement note disclosures, to what extent did your SOX compliance team identify plausible risks that could threaten the integrity of the information in each one of the note disclosures?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain

19. To what extent did your SOX compliance team identify plausible IT-related risks (e.g., infrastructure, access, integrity, security etc.) for each application that impacts financial statement accounts and note disclosures?

- O No extent
- O Some extent
- O Moderate extent
- O Large extent
- O Uncertain

20. Indicate the extent to which each of the following factors contributed to any excess costs associated with SOX 302/404 compliance initiative in your organization. [Cost includes hard dollar outlays and the opportunity costs of delayed innovation, focus away from value-adding activities, etc.].

Potential Cost Factors	No extent	Some extent	Moderate extent	Large extent	Uncertain
1. Lack of a generally accepted assessment criteria/framework available while evaluating the effectiveness of our system of internal controls	O	O	O	O	O
2. Difficulty in using the COSO 1992 framework in arriving at a consensus opinion on the effectiveness of our system of internal controls	O	O	O	O	O
3. Our external auditors' insistence on documenting and testing all processes irrespective of the residual risk profile of these processes	O	O	O	O	O
4. Lack of practical guidance from the SEC or other professional organizations on how to accomplish the task of deciding what constitutes an "effective or ineffective" internal control system	O	O	O	O	O
5. Lack of practical guidance from SEC on what exactly is a "significant deficiency vs. material control weakness"	O	O	O	O	O
6. Redundant testing performed by external auditors and internal auditors or SOX compliance group due to the inability of these groups to collaborate to reduce the sample size	O	O	O	O	O

END OF SECTION II

SECTION III: 1992 COSO FRAMEWORK SPECIFIC QUESTIONS

21. Prior to the enactment of the Sarbanes-Oxley Act of 2002, to what extent was your organization formally utilizing the guidance provided by the COSO 1992 framework to effectively manage its enterprise risk and controls?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Not sure

22. Prior to the enactment of the Sarbanes-Oxley Act of 2002, to what extent were your external auditors formally utilizing the guidance provided by the COSO 1992 framework to "size-up" the effectiveness of your organization's system of internal control and sharing their assessment annually with your company via the management letter?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Not sure

23. Prior to the enactment of the Sarbanes-Oxley Act of 2002, to what extent was the internal audit function in your organization formally utilizing the guidance provided by the COSO 1992 framework to "size-up" the effectiveness of your organization's system of internal control and sharing this assessment on a periodic basis with the company management and the audit committee?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Not sure

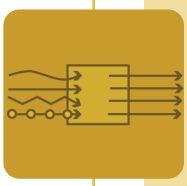
24. When assessing the effectiveness of your internal controls over IT to comply with SOX 302/404 requirements, which framework or standard did your organization use? (You may choose more than one response).
    - O COBIT
    - O ITGI-A subset of the COBIT
    - O COSO 1992
    - O COSO ERM
    - O ISO 17779
    - O Uncertain
    - O Other framework (please specify)

25. When evaluating and assessing the effectiveness of your internal control over financial reporting (excluding IT controls) to comply with SOX 302/404 requirements, which "dominant" internal control framework or standard did your organization use?
    - O COSO 1992 framework, *Internal Control—Integrated Framework*
    - O COSO ERM framework, *Enterprise Risk Management—Integrated Framework*
    - O Criteria of Control (CoCo) framework issued by the Canadian Institute of Chartered Accountants
    - O Turnbull framework, *Internal Control: Guidance for Directors on the Combined Code,* issued by the Institute of Chartered Accountants in England and Wales
    - O Uncertain
    - O Other framework (please specify)

26. In your opinion, using the COSO 1992 control framework, to what extent is it possible to arrive at a reliable pass or fail conclusion on the effectiveness of an entity's system of internal control over external financial reporting (i.e., one that can be replicated by two independent assurance professionals within a narrow margin of error)?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain

27. In your opinion, using the COSO 1992 control framework, to what extent is it possible to achieve a high level (90% or above) of consensus between company management and their external auditors while opining on the effectiveness of a client's system of internal control under Sections 302/404 when each conducts its assessment on an independent basis?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain

28. In your opinion, to what extent does the COSO 1992 control framework provides specific guidance (as opposed to "motherhood and apple-pie" type of guidance on elements of an internal control system) to all those who are responsible for assessing and concluding on the effectiveness of a company's system of internal control over financial reporting?
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain



29. When evaluating internal controls related to most of your specific account balances to what extent did your SOX compliance team specifically rely on the guidance provided by the COSO 1992 framework for each one of the five COSO components of internal control?

	No extent	Some extent	Moderate extent	Large extent	Uncertain
1. Control Environment	O	O	O	O	O
2. Risk Assessment	O	O	O	O	O
3. Control Activities	O	O	O	O	O
4. Information and Communication	O	O	O	O	O
5. Monitoring	O	O	O	O	O

30. When evaluating internal controls related to most of your note disclosures to what extent did your SOX compliance team specifically rely on the guidance provided by the COSO 1992 framework for each one of the five COSO components of internal control?

	No extent	Some extent	Moderate extent	Large extent	Uncertain
1. Control Environment	O	O	O	O	O
2. Risk Assessment	O	O	O	O	O
3. Control Activities	O	O	O	O	O
4. Information and Communication	O	O	O	O	O
5. Monitoring	O	O	O	O	O

31(a). Did you complete the mandatory antifraud assessment for industry specific risk factors required by PCAOB auditing standard #2?

O Yes
O No

If No, go to Question 32(a).

31(b). When completing the mandatory antifraud assessment for industry specific risk factors, required by PCAOB Auditing Standard #2, to what extent did your SOX compliance team specifically rely on the guidance provided by the COSO 1992 framework for each one of the five COSO components of internal control?

	No extent	Some extent	Moderate extent	Large extent	Uncertain
1. Control Environment	O	O	O	O	O
2. Risk Assessment	O	O	O	O	O
3. Control Activities	O	O	O	O	O
4. Information and Communication	O	O	O	O	O
5. Monitoring	O	O	O	O	O

32(a). Did you evaluate macro-level antifraud controls (other than the mandatory antifraud assessment for industry specific risks as asked in the previous question) while complying with section 404 of the Sarbanes-Oxley Act of 2002?

O Yes
O No

If No, go to Question 33(a).

32(b). When evaluating macro-level antifraud controls (other than the mandatory antifraud assessment for industry specific risks as asked in the previous question) to what extent did your SOX compliance team specifically rely on the guidance provided by the COSO 1992 framework for each one of the five COSO components of internal control?

	No extent	Some extent	Moderate extent	Large extent	Uncertain
1. Control Environment	O	O	O	O	O
2. Risk Assessment	O	O	O	O	O
3. Control Activities	O	O	O	O	O
4. Information and Communication	O	O	O	O	O
5. Monitoring	O	O	O	O	O

33(a). Did you evaluate IT Governance and General IT Controls while complying with section 404 of the Sarbanes-Oxley Act of 2002?

O Yes
O No

If No, go to Question 34(a).

33(b). When evaluating IT Governance and General IT Controls to what extent did your SOX compliance team specifically rely on the guidance provided by COSO 1992 framework for each one of the five COSO components of internal control? If you believe a certain COSO element does not apply to the IT Governance and General IT Controls, please choose not applicable.

	No extent	Some extent	Moderate extent	Large extent	Uncertain
1. Control Environment	O	O	O	O	O
2. Risk Assessment	O	O	O	O	O
3. Control Activities	O	O	O	O	O
4. Information and Communication	O	O	O	O	O
5. Monitoring	O	O	O	O	O

34(a). Did you evaluate IT Application Controls while complying with section 404 of the Sarbanes-Oxley Act of 2002?

O Yes
O No

If No, go to Question 35.

34(b). When evaluating IT Application Controls to what extent did your SOX compliance team specifically rely on the guidance provided by COSO 1992 framework for each one of the five COSO components of internal control? If you believe a certain COSO element does not apply to the IT Application Controls, please choose not applicable.

	No extent	Some extent	Moderate extent	Large extent	Uncertain
1. Control Environment	O	O	O	O	O
2. Risk Assessment	O	O	O	O	O
3. Control Activities	O	O	O	O	O
4. Information and Communication	O	O	O	O	O
5. Monitoring	O	O	O	O	O

35. In your opinion, is it necessary to "map" all discovered control deficiencies to one or more of the five COSO components to claim that your organization conducted its internal control assessment "in accordance with the COSO 1992 framework"?

- O No, it is not essential to map all discovered control deficiencies to COSO components to make such a claim.
- O As long as an entity can demonstrate that it actively evaluated all five COSO components at the entity-level, it is reasonable and sufficient to make such a claim.
- O Yes, it is absolutely essential to clearly map all discovered control deficiencies to relevant COSO components to make such a claim.
- O Uncertain.

36. Did your SOX compliance team "map" all of the discovered control deficiencies to one or more of the five COSO components as part of the process of forming an opinion on the effectiveness of your organization's internal controls?

- O No, we did not "map" any of the discovered control deficiencies to any one of the COSO components.
- O Yes, we only "mapped" some of the discovered control deficiencies to all the applicable COSO components.
- O Yes, we clearly "mapped" all of the discovered control deficiencies to all the applicable COSO components.
- O We did not need to "map" the discovered control deficiencies to the five COSO components because during the documentation process we had already "mapped" all of the controls to applicable COSO components.
- O Uncertain.

37. In your opinion, to what extent did such a mapping result in operational improvements to the management of risks and controls in your organization?

    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain

38. Overall, to what extent is the guidance provided in the COSO 1992 framework helpful in assisting and guiding your SOX team in "mapping" the discovered control deficiencies to one or more of COSO's five components as part of the process of forming an opinion on the effectiveness of your company's internal controls?

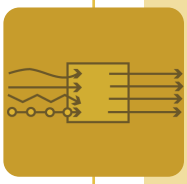
    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain

39. To what extent did your SOX compliance team, at the entity level, evaluate the overall effectiveness of each one of the five components of the COSO framework as part of the process of forming an opinion on the effectiveness of your organization's internal controls?

    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain

40. The SEC's Final Rules implementing Section 404 state that "Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the registrant's internal control over financial reporting." AS2 requires the same conclusion from the external auditors. In other words, this requirement essentially sets the pass/fail criteria. In the absence of such a specific requirement, in your opinion, to what extent is it possible for management as well as external auditors, to form a pass/fail opinion on the effectiveness of internal control over financial reporting solely based on the guidance provided by the COSO 1992 control framework?

    - O No extent
    - O Some extent
    - O Moderate extent
    - O Large extent
    - O Uncertain



41. In your opinion, which one of the following 2 statements is “more true” for your first-year SOX certification efforts?
    - O Majority of our internal control assessment was largely guided by and conducted in accordance with the PCAOB Auditing Standard No. 2.
    - O Majority of our internal control assessment was largely guided by and conducted in accordance with the COSO 1992 internal control framework.

42. Paragraph 13 of the PCAOB Auditing Standard No. 2 lays very specific criteria for an acceptable control model. These criteria are reproduced below in the left hand column. In your opinion, to what extent, each one of these criteria is fulfilled by the 1992 COSO control framework?

    "In addition to being available to users of management’s reports, a framework is suitable only when it..."

	No extent	Some extent	Moderate extent	Large extent	Uncertain
1. Is free from bias	O	O	O	O	O
2. Permits reasonably consistent qualitative and quantitative measurements of a company’s internal control over financial reporting	O	O	O	O	O
3. Is sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of a company’s internal control over financial reporting are not omitted	O	O	O	O	O
4. Is relevant to an evaluation of internal control over financial reporting	O	O	O	O	O

END OF SECTION III

SECTION IV: SOX SKILL-SET RELATED QUESTIONS

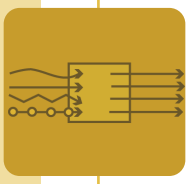
43. In your opinion, what do you think is your individual level of competency in applying the COSO framework to conduct an assessment of internal controls over financial reporting for SOX 302/404 certification purposes?

- O I am an expert in applying the COSO 1992 framework in my company.
- O I am not an expert in applying the COSO 1992 framework but I can make it work.
- O I am somewhat unfamiliar with how to really apply the COSO 1992 framework.
- O I really struggle with applying the COSO 1992 framework.
- O I am uncertain about my level of competency in applying COSO 1992.

44. In your opinion, to what extent are the following skills and related knowledge important to cost-effective SOX compliance in members of a SOX implementation team? Please note that in this question you are not to focus on the effectiveness of any of the frameworks or the standards or the regulations rather focus on the level of competency to apply current guidance to do what needs to be done to become SOX compliant?

	No extent	Some extent	Moderate extent	Large extent	Absolutely Essential
1. Being able to understand and apply existing risk-models	O	O	O	O	O
2. Being able to understand and apply current control models (such as COSO 1992, COSO ERM, etc.) that are the dominant models for SOX 404 reporting	O	O	O	O	O
3. Being able to understand and apply the control model that my CEO/CFO uses to report against under Section 302 of the SOX	O	O	O	O	O
4. Being able to reasonably assess the "residual risk status" associated with various financial statement accounts and note disclosures	O	O	O	O	O
5. Being able to determine in a most efficient manner the key controls in my organization	O	O	O	O	O
6. Being able to create relevant process flowcharts and narratives with needed information	O	O	O	O	O

7. Being able to determine how much internal control testing is necessary to conclude whether we have an effective system of internal control over financial reporting	O	O	O	O	O
8. Being able to correctly identify underlying internal control weaknesses by examining discovered control exceptions	O	O	O	O	O
9. Being able to correctly grade discovered internal control deficiencies as a significant control deficiency or a material control weakness	O	O	O	O	O
10. Being able to evaluate the discovered control deficiencies by identifying the relevant aggregation criteria	O	O	O	O	O
11. Being able to understand and apply numerous other requirements of the AS2 to ensure that my company is in compliance with SOX 302/404	O	O	O	O	O
12. Being able to independently conduct a risk and control self-assessment	O	O	O	O	O
13. Being able to evaluate the reliability of self-assessment information produced by process/ account owners	O	O	O	O	O
14. Being able to determine the cost vs. benefit of obtaining additional assurance on my company's system of internal control over financial reporting	O	O	O	O	O
15. Being able to use the skills learned through SOX to competently identify and assess the risks and controls in other areas such as safety, regulatory compliance, product quality, cost control, etc.	O	O	O	O	O



45. In your opinion, to what extent are the following skills and related knowledge important to cost-effective SOX compliance in an external audit team conducting SOX 302/404 work?

	No extent	Some extent	Moderate extent	Large extent	Absolutely Essential
1. Being able to understand and apply existing risk-models	O	O	O	O	O
2. Being able to understand and apply current control models (such as COSO 1992, COSO ERM, etc.) that are the dominant models for SOX 404 reporting	O	O	O	O	O
3. Being able to understand and apply the control model that my CEO/CFO uses to report against under Section 302 of the SOX	O	O	O	O	O
4. Being able to reasonably assess the "residual risk status" associated with various financial statement accounts and note disclosures	O	O	O	O	O
5. Being able to determine in a most efficient manner the key controls in my organization	O	O	O	O	O
6. Being able to create relevant process flowcharts and narratives with needed information	O	O	O	O	O
7. Being able to determine how much internal control testing is necessary to conclude whether we have an effective system of internal control over financial reporting	O	O	O	O	O
8. Being able to correctly identify underlying internal control weaknesses by examining discovered control exceptions	O	O	O	O	O
9. Being able to correctly grade discovered internal control deficiencies as a significant control deficiency or a material control weakness	O	O	O	O	O
10. Being able to evaluate the discovered control deficiencies by identifying the relevant aggregation criteria	O	O	O	O	O

11. Being able to understand and apply numerous other requirements of the AS2 to ensure that my company is in compliance with SOX 302/404	O	O	O	O	O
12. Being able to independently conduct a risk and control self-assessment	O	O	O	O	O
13. Being able to evaluate the reliability of self-assessment information produced by process/ account owners	O	O	O	O	O
14. Being able to determine the cost vs. benefit of obtaining additional assurance on my company's system of internal control over financial reporting	O	O	O	O	O
15. Being able to use the skills learned through SOX to competently identify and assess the risks and controls in other areas such as safety, regulatory compliance, product quality, cost control, etc.	O	O	O	O	O

46. In your opinion, to what extent are the following skills and related knowledge important to cost effective SOX compliance in a consultant advising on SOX 302/404 certification?

	No extent	Some extent	Moderate extent	Large extent	Absolutely Essential
1. Being able to understand and apply existing risk-models	O	O	O	O	O
2. Being able to understand and apply current control models (such as COSO 1992, COSO ERM, etc.) that are the dominant models for SOX 404 reporting	O	O	O	O	O
3. Being able to understand and apply the control model that my CEO/CFO uses to report against under Section 302 of the SOX	O	O	O	O	O
4. Being able to reasonably assess the "residual risk status" associated with various financial statement accounts and note disclosures	O	O	O	O	O

5. Being able to determine in a most efficient manner the key controls in my organization	O	O	O	O	O
6. Being able to create relevant process flowcharts and narratives with needed information	O	O	O	O	O
7. Being able to determine how much internal control testing is necessary to conclude whether we have an effective system of internal control over financial reporting	O	O	O	O	O
8. Being able to correctly identify underlying internal control weaknesses by examining discovered control exceptions	O	O	O	O	O
9. Being able to correctly grade discovered internal control deficiencies as a significant control deficiency or a material control weakness	O	O	O	O	O
10. Being able to evaluate the discovered control deficiencies by identifying the relevant aggregation criteria	O	O	O	O	O
11. Being able to understand and apply numerous other requirements of the AS2 to ensure that my company is in compliance with SOX 302/404	O	O	O	O	O
12. Being able to independently conduct a risk and control self-assessment	O	O	O	O	O
13. Being able to evaluate the reliability of self-assessment information produced by process/ account owners	O	O	O	O	O
14. Being able to determine the cost vs. benefit of obtaining additional assurance on my company's system of internal control over financial reporting	O	O	O	O	O

15. Being able to use the skills learned through SOX to competently identify and assess the risks and controls in other areas such as safety, regulatory compliance, product quality, cost control, etc.	O	O	O	O	O

47. In the space provided below, based on your personal experience please tell us which skills and related knowledge are most critical to effectively complete a SOX compliance project?

END OF SURVEY

THANK YOU FOR TAKING THE TIME TO COMPLETE THIS SURVEY

NOTE: Two additional questions dealt with time taken to complete the survey and whether the survey participant would like to receive a summary of the results.