Use of COSO 1992 in Management Reporting on Internal Control

THE COSO FRAMEWORK provides an integrated framework that identifies components and objectives of internal control. But does it set forth detailed guidance as to the steps that management must follow in assessing the effectiveness of a company's internal controls over financial reporting?

By Parveen P. Gupta and Jeffrey C. Thomson

For the first time in the history of corporate financial reporting and disclosure, per Section 404 of the Sarbanes-Oxley Act of 2002 (SOX), company management and their external auditors are required to report on the state of internal controls over financial reporting (ICoFR). Companies must include these opinions in the quarterly and annual financial disclosures they file with the U.S. Securities & Exchange Commission (SEC). At the same time, the SEC Final Rules about implementing Section 404 also require that a registrant disclose all "significant control deficiencies" to its audit committee as well as its external auditors and disclose all "material control weaknesses" in its ICoFR to the public via its periodic filings with the SEC. Not an easy task, and, in many cases, it's a huge undertaking.

The SEC requires management and external auditors to use an internal control framework that meets its criteria specified in Section II.B.3a of the Section 404 Final Rules. While acknowledging the other control frameworks—the Guidance on Assessing Control from the Canadian Institute of Chartered Accountants and the Turnbull Report by the Institute of Chartered Accountants in England and Wales—the Final Rules explicitly state that the COSO Framework satisfies SEC criteria and "may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements" by companies listed on U.S. stock exchanges. In the SOX compliance world, this endorsement is widely understood to refer to the 1992 *Internal Control—Integrated Framework* that was issued by COSO, or the Committee of Sponsoring Organizations of the Treadway Commission. (The formal name of the Treadway Commission is the National Commission on Fraudulent Financial Reporting. James C. Treadway, Jr., was its first chairman, hence the informal name. COSO was formed in 1985 to sponsor the Commission, an independent private-sector initiative that studied the factors that could lead to fraudulent financial reporting and that developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.)

Since management reporting on internal control provisions kicked in for companies with fiscal years ending on or after November 15, 2004, a number of reports and surveys have documented the enormous compliance costs U.S.-listed companies are incurring in their quest to certify the integrity of ICoFR. Many of these surveys and reports have criticized the way external auditors have implemented Section 404 requirements when using Auditing Standard No. 2 (AS2) from the Public Company Accounting Oversight Board (PCAOB).

In an effort to make implementation less onerous by understanding concerns of the registrants, external auditors, and the investing community in general, the SEC and the PCAOB have held two roundtables and issued additional clarifications and guidance on AS2, which is the primary auditing standard for external auditors to follow in their internal control assessment evaluations. Most concerns and regulatory remediation efforts have centered on shifting the external auditors' focus from a bottom-up, control-centric approach to a top-down, risk-based approach to assessing and certifying the effectiveness of a company's internal controls. But comment letters filed with the SEC and experience working with clients implementing Section 404 requirements indicate that the registrants are also struggling to implement the five components of the COSO 1992 Control Framework: control environment, risk assessment, control activities, information and communication, and monitoring.

Table 1: Use of the COSO 1992 Framework Prior to SOX

RESPONSE SCALE	BY COMPANY MANAGEMENT TO MANAGE ITS ENTERPRISE RISK AND CONTROLS	BY INTERNAL AUDITORS TO SIZE UP THE EFFECTIVENESS OF THE COMPANY'S INTERNAL CONTROLS
1. No Extent	37.8%	33.5%
2. Some Extent	31.4%	24.1%
3. Moderate Extent	13.9%	17.7%
4. Large Extent	11.3%	15.3%
5. Uncertain	5.6%	9.4%

To investigate these concerns, the Institute of Management Accountants (IMA®), one of COSO's five sponsoring organizations, commissioned Parveen P. Gupta of Lehigh University to conduct a study. The research took place in the fourth quarter of 2005 and early 2006, and IMA is publishing the report this month. The study focused on current usage, the role of, and the extent of guidance the COSO 1992 Framework provides in helping management conduct its internal control evaluation. It also covered several other areas, such as cost of compliance; accountabilities for Section 404 work; use of top-down, risk-based assessment; assessing fraud risk vulnerability; IT controls; and skill sets needed to complete Section 404 assessment cost effectively. (For information on how to order the IMA study, visit www.imanet.org.)

We surveyed members of IMA and the Institute of Internal Auditors (IIA), ultimately collecting data from 374 respondents. They are internal auditors (39%), SOX implementation specialists and accounting managers (23%), controllers and assistant controllers (16%), and vice presidents (10%). The remaining 12% are CFOs, audit committee chairs, compliance directors, SOX steering committee members, etc. About 75% have one or more of the formal accounting and auditing certifications, such as Certified Public Accountant (CPA), Certified Management Accountant (CMA®), Certified Internal Auditor (CIA), etc. Based on the demographics, we have a well-seasoned group of respondents. In fact, more than 70% have an

overall work experience of 15 years or more, and about 60% of these have been in their current position from one to five years. More than two-thirds of the survey participants have spent more than 20% of their time working on SOX 302/404 compliance-related activities.

Besides presenting the findings for the entire sample, the research study also analyzes the data by company size (small and medium-to-large) and job title (management vs. internal auditors). Here we will highlight some areas related to how management is using the COSO 1992 Control Framework in their efforts to assess and certify the effectiveness of their company's internal controls over financial reporting.

You might think that a significant number of companies would use the **COSO 1992 FRAMEWORK** guidance to manage their enterprise's risks and controls as well as size up their internal control system. This isn't the case.

RELIANCE ON COSO

As we indicated earlier, the COSO 1992 Framework is the accepted framework for Section 404 implementation. It was issued in response to the recommendations of the Treadway Commission's 1987 report that suggested the sponsoring organizations work together to develop integrated guidance on internal control. The report presented a common definition of internal control and a framework against which internal control systems could be assessed and improved. The circumstances surrounding internal control breakdowns then were no different from the environment today. Given the importance of good internal controls that the COSO 1992 Framework espouses and the considerable amount of time that it has been out in the market, you might think that a significant number of companies would use its guidance to manage their enterprise's risks and controls as well as size up their internal control system. This isn't the case. Table 1 indicates that, prior to SOX, use of the COSO 1992 Framework on both of these dimensions was somewhat minimal. Only 11% of the respondents believe that their company used the COSO 1992 Framework to a large extent to manage its risks and controls. What's more, only 15% believe that their internal auditors used the COSO 1992 Framework to a large extent to size up the effectiveness of the company's internal controls. According to the respondents, some reasons for limited use of the Framework were lack of management awareness of it, limited use of the risk-assessment component for internal audit scoping decisions, and more.

When asked "Which is actually guiding the internal control assessments, COSO 1992 or AS2?" an overwhelming 62% chose AS2. These results simply reaffirm what many critics of the Section 404 implementation process have been saying: In the absence of specific SEC guidance, AS2 has become the de facto standard for management to assess and report on internal control effectiveness. Recall that AS2 is an auditing standard that provides guidance to the external auditors on how they should audit management's assessment of a company's internal control effectiveness.

Table 2 shows how much the survey participants relied on the five COSO components while evaluating internal controls over specific account balances. Actually, only one-third of the survey respondents believe that the com-

Table 2: Reliance on Five COSO Components to Evaluate Controls over Specific Account Balances

FIVE COMPONENTS OF THE COSO 1992 FRAMEWORK	NO EXTENT	SOME EXTENT	MODERATE EXTENT	LARGE EXTENT	UNCERTAIN
1. Control Environment	6%	28%	31%	31%	4%
2. Risk Assessment	7%	32%	34%	23%	4%
3. Control Activities	4%	23%	30%	39%	4%
4. Information and Communication	7%	36%	28%	23%	6%
5. Monitoring	6%	31%	31%	27%	4%

Table 3: Perceptions about COSO 1992 Meeting the SEC Criteria of Suitability

CRITERIA FOR AN ACCEPTABLE CONTROL EVALUATION FRAMEWORK PER SECTION 404 FINAL RULES	NO EXTENT	SOME EXTENT	MODERATE EXTENT	LARGE EXTENT	UNCERTAIN
1. Is free from bias	2%	23%	28%	36%	11%
2. Permits reasonably consistent qualitative and quantitative measurements of a company's internal control over financial reporting	5%	25%	28%	34%	8%
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%	25%	27%	36%	9%
4. Is relevant to an evaluation of internal control over financial reporting	2%	22%	27%	40%	9%

ponents provide them with sufficient guidance during their evaluations. Let's focus on the "large extent" responses. We find that 39% cited the control activities component, 31% cited the control environment component, 27% cited the monitoring component, and 23% cited the risk assessment as well as the information and communication components.

Interestingly, even when we factor in the "moderate extent" responses or conversely focus only on the "no extent" and "some extent" responses, the guidance provided in the five COSO components doesn't "conclusively" emerge as dominating managements' assessments.

Here are some written comments from the respondents that indicate SOX compliance teams face considerable challenges using the COSO 1992 Framework:

- *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.*
- *For the control activities, the compliance team was obliged to follow the control framework provided by our external auditors.*

SUITABILITY OF THE COSO 1992 FRAMEWORK

As we mentioned earlier, the SEC has clearly indicated that, in the U.S., the COSO 1992 Framework satisfies its criteria for management to use when implementing Section 404. Indeed, the Commission's directive has been followed to the letter of the law. Our review of management reports on internal control filed with the Commission under Item 9A of most 10-K forms reveals that almost all the companies are unequivocally claiming that they conduct their internal control evaluation in accordance with the COSO 1992 Framework.

But given that the survey participants aren't overwhelmingly relying on the COSO 1992 guidance, we sought to gauge their perceptions about the Framework's suitability in light of the SEC's four specific criteria. These results appear in Table 3.

Overall, when we focus on just the "large extent" response category, the results in Table 3 indicate that only about one of every three survey participants believes COSO 1992 meets the SEC's "suitability" criteria. Since the COSO 1992 Control Framework has emerged as the most often cited framework in management reports filed with the SEC, you'd expect much stronger sentiment and a broader acknowledgment of its meeting the SEC criteria. Interestingly, even after considering the "moderate extent" responses, we find that still only about one in every four survey participants believes that COSO 1992 passes on the four criteria.

Of particular concern are the low response rates on criteria #2 and #3, which respectively require that a suitable control framework for Section 404 compliance be (1) capable of producing consistent measurements of a

Smaller public companies with fewer than 1,000 employees have a less favorable impression of the COSO 1992 FRAMEWORK along the four dimensions.

Table 4: Can COSO 1992 Guidance Alone Lead to a Pass/Fail Conclusion?

RESPONSE SCALE	% OF THE TOTAL SAMPLE	INTERNAL AUDITORS	MANANGEMENT TYPES
1. No Extent	14.6%	14.3%	14.9%
2. Some Extent	42.5%	41.4%	43.5%
3. Moderate Extent	24.6%	24.1%	25.0%
4. Large Extent	12.6%	16.5%	9.5%
5. Uncertain	5.6%	3.8%	7.1%

Table 5: Is It Possible to Arrive at a Reliable Pass/Fail Conclusion on ICoFR Using COSO 1992?

RESPONSE SCALE	% OF THE TOTAL SAMPLE	SMALL COMPANIES	MEDIUM-TO-LARGE COMPANIES
1. No Extent	2.4%	0.0%	3.0%
2. Some Extent	49.8%	58.1%	47.9%
3. Moderate Extent	18.0%	16.1%	18.5%
4. Large Extent	22.0%	16.1%	23.4%
5. Uncertain	7.6%	9.7%	7.2%

company's ICoFR and (2) sufficiently complete so that all relevant factors that could potentially alter a conclusion about the effectiveness of ICoFR aren't omitted from evaluation. When we further evaluate the data by company size, we find that smaller public companies with fewer than 1,000 employees have a less favorable impression of the COSO 1992 Framework along the four dimensions.

To understand such a low level of acceptance on SEC criteria #2 and #3, we further explored the survey participants' experiences with using the COSO 1992 Framework. Since complying with Section 404 requires a pass/fail conclusion about the effectiveness of ICoFR, we should be able to make such a determination based solely on COSO 1992 as an underlying control model. Table 4 contains the results from the following question:

"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?"

When focusing just on the "large extent" response category, only 13% believe that the COSO 1992 Framework, in the absence of direction from AS2, provides sufficient guidance to unequivocally conclude whether a company's ICoFR is effective. By job category, more internal auditors (17%) than management types (10%) indicate that COSO 1992 alone can lead to such a conclusion. Even if we include the "moderate extent" responses, there are still significant doubts about the "sufficiently complete" attribute that SEC criterion #3 specifies. Of course, we also asked many questions about applying the guidance provided by the COSO 1992 Framework to evaluate internal controls over note disclosures, assess fraud risk vulnerability, and evaluate IT controls. And the opinions of the survey participants don't change significantly. Their doubts are manifested in some of the written comments:

- *COSO is very vague and nonspecific. Even the training classes in COSO cannot answer the what-to-do questions asked by auditors.*
- *It was too high-level. Not enough detail, which caused much confusion and caused a lot of unnecessary money to be spent in the interpretation.*

We further explored the requirement embedded in the SEC criterion #2 by asking survey respondents two additional questions. Table 5 presents the answers to the first question:

"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)?"

Focusing on the "no extent" and "some extent" responses, more than half believe it isn't possible to arrive at a reliable pass/fail conclusion about the effectiveness of an entity's ICoFR using the COSO 1992 Framework. When we analyzed the data by company size, there appeared to be slight differences in the perceptions of the

participants. Fewer survey participants from small companies chose the response categories of "moderate" to "large" extent, indicating that smaller companies are more negative about the COSO 1992 Framework.

Table 6 contains the responses to the second question: "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?"

Since compliance with Section 404 requires separate assessments by company management and its external auditors, it's important that the two groups form a consensus on the effectiveness of a company's ICoFR when each conducts its evaluation using the same control framework. Only 36% of the survey participants think that achieving such a consensus is feasible from a moderate to a large extent while using the COSO 1992 Framework. When we examined the same data by job title, we found slightly more internal auditors (about 39%) than management types (approximately 34%) believe that a high degree of consensus is feasible. Similarly, when we examined the data by company size, nearly 60% of small companies and 52% of medium-to-large companies chose the response categories of "no extent" to "some extent," indicating once again that, based on this question, smaller public companies have a more negative impression of the COSO 1992 Framework.

Tables 5 and 6 lend credibility to the low response rates accorded to the SEC criterion #2 as reported in Table 3. Overall, these findings indicate that the COSO 1992 Framework may be unable in practice to produce reasonably consistent qualitative and quantitative measurements of a company's ICoFR.

Table 6: Consensus in Conclusions between Management and External Auditors Using COSO 1992

RESPONSE SCALE	% OF THE TOTAL SAMPLE	SMALL COMPANIES	MEDIUM-TO-LARGE COMPANIES
1. No Extent	3.1%	1.6%	3.4%
2. Some Extent	50.8%	58.1%	49.1%
3. Moderate Extent	18.7%	19.4%	18.5%
4. Large Extent	17.7%	12.9%	18.9%
5. Uncertain	9.8%	8.1%	10.2%

THE LACK OF SKILLS and a practical assessment methodology is a dangerous mix when it comes to opining on the effectiveness of a company's ICoFR.

APPROPRIATE SKILL SETS

Although it was the Cohen Commission Report in 1978 that called for management to own internal controls, experience indicates that, until the passage of SOX, internal auditors were the dominant group involved in documenting, assessing, and reporting on an entity's system of internal control. The role of the finance and controllership staff in this important activity was often very limited because of staff shortages, the rush to meet the ever-shortening regulatory quarterly filing deadlines, an increasing number of GAAP pronouncements to track, and the like.

Similarly, external auditors stopped developing these skills in their staff. The reason? To earn a sustainable margin in a largely commoditized financial audit market, they set the control risk to 100% and focused only on substantive testing to opine on the fairness of a client's financial statements. The overall result of decades of not paying attention to a company's risk and control environment is now a severe shortage of accounting and auditing professionals with a sufficient skill set to cost effectively complete internal control evaluations as Section 404 mandates. Table 7 captures individual competency levels in applying the COSO 1992 guidance.

Not surprisingly, only 24% consider themselves experts in applying the COSO 1992 Framework to evaluate ICoFR in their company. But nearly 60% feel that they can "make it work." The lack of skills and a practical assessment methodology is a dangerous mix when it comes to opining on the effectiveness of a company's ICoFR, whether the opinion comes from management or external auditors.

ENORMOUS POTENTIAL

Certainly the regulatory bodies can't do anything about developing necessary skills in the SOX compliance

Table 7: Level of Individual Competency in Applying COSO 1992 Guidance

LEVEL OF COMPETENCE	# 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 exert 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 am uncertain about my level of competency in applying the COSO 1992 Framework.	13	4.6%

workforce. This is left largely to the institutions of higher education and professional certification-granting bodies such as IMA, the Institute of Internal Auditors (IIA), and the American Institute of CPAs (AICPA). Yet the SEC has recently recognized that, among others, one reason the registrant community isn't getting the SOX 404 compliance right is perhaps due to the lack of guidance to management regarding evaluating an entity's ICoFR. According to SEC Chairman Christopher Cox, "Auditing Standard No. 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 AS2."

Additionally, in its July 11, 2006, Concept Release, the SEC observes that: "While the COSO framework provides an integrated framework that identifies components and objectives of internal control, it does not set forth detailed guidance as to the steps that management must follow in assessing the effectiveness of a company's ICoFR. We, therefore, distinguish between the COSO framework as an internal control framework and other forms of guidance that illustrate how to conduct an assessment of the effectiveness of ICoFR."

Taken together, the findings of this research study and the above-mentioned statements from the SEC indicate that the COSO 1992 Framework may be falling short of providing the much-needed implementation guidance to company managements for assessing and reporting on internal controls. Perhaps issuing specific implementation guidance or an internal control assessment framework that would complement or supplement the largely principles-based guidance of the COSO 1992 Framework would finally silence the critics of the Section 404 requirements. The Sarbanes-Oxley Act of 2002 is the right piece of legislation that has enormous potential to enhance control governance in the U.S. capital markets. This is if—and *only* if—we can get the much-needed implementation of Section 404 right. ■

Parveen P. Gupta, LLB, Ph.D., is the Frank L. Magee Distinguished Professor of Accounting in the College of Business and Economics at Lehigh University in Bethlehem, Pa. You can reach Parveen at (610) 758-3443 or ppg0@lehigh.edu.

Jeffrey C. Thomson is vice president of research and applications development for the IMA. You can reach Jeff at (201) 474-1586 or jthomson@imanet.org.