

ENTERPRISE RISK AND CONTROL

EXECUTIVE SUMMARY

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



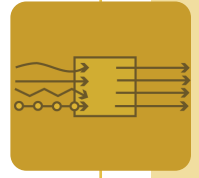
ENTERPRISE RISK AND CONTROL

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,



ENTERPRISE RISK AND CONTROL

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.