



600 N. Plankinton Ave.
Milwaukee, WI 53201-3005
t: 414-272-8575
800-248-1946
f: 414-272-1734
www.asq.org

February 23, 2007

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

Re: File Number S7-24-06
Subject: Comments on Draft SEC / PCAOB SOX Proposals

Dear Ms. Morris:

The American Society for Quality (ASQ) is pleased to submit the attached comments on the SEC's proposed rule regarding management evaluation of internal control over financial reporting.

ASQ recognizes the importance of the Sarbanes-Oxley Act (SOX) to the global economy and the role it plays for investors by providing transparency in organizational finances. To this end, in 2004 ASQ instituted a new organization, the Sarbanes-Oxley (SOX) Community. The goal of this community is to provide dialogue in understanding the role quality and environmental management systems can play in supporting organizations' compliance to the Act.

Much of the dialogue has centered on Section 404 of the Act. The requirement that organizations must have and be able to demonstrate an effective system of control led to research of various methods of providing effective quality and environmental management systems. The Community reviewed the Malcolm Baldrige Award criteria, the Six Sigma methodology and the ISO standards ISO 9001:2000 and ISO 14001:2004. The ISO standards were selected as a pair because of their closeness to the structure of the COSO guidance used by most organizations to satisfy Section 404 and because many public companies are registered to ISO 9001 and 14001.

With this background in mind, the Community formed a "SOX Team" to review the recent SEC and PCAOB draft documents published on December 19, 2006. We applaud your efforts to re-focus industry responses to a "risk-based, top down approach." The result will be that organizations will focus on the key controls which can indicate the possibility of material misstatements in financial statements. This will surely reduce the cost of compliance, but will also allow an organization to focus on its important business processes. It will also foster the use of quality improvement tools on these processes and will result in a more effective operation of the organization.

A major part of the SOX Team effort has been to look for ways of "building quality" into the development of financial reports. Our review of your December 19 publications has given us an opportunity to put specificity on this term. The SOX Team has found

opportunities in the two documents which include the following key practices of the quality and environmental communities:

- Continual improvement techniques
- The use of data analysis to identify and correct potential risks
- Methodology for assuring personnel competence
- Controls to manage an organization's documentation and records
- Clarification of management's roles and responsibilities.

The American Society for Quality would like to applaud your efforts to reduce the impact of Sarbanes-Oxley on industry and your special attention to small businesses. Quality practices have been very important to small organizations because the reduced staff in these organizations make their effective operation crucial. It is also proper that external auditors use the work of others, including procedures and records of internal quality and environmental managers, engineers, and auditors.

I would like to offer the services of the SOX Team to support your future efforts. We recognize the great importance of Sarbanes-Oxley to the well being of our country and are quite willing to help as your committees move forward.

Thank you,



Ronald D. Atkinson
President
American Society for Quality

Attachment: The American Society for Quality Sarbanes-Oxley Team Comments on "Management's Report on Internal Control over Financial Reporting"

About the American Society for Quality

The American Society for Quality (www.asq.org) is the world's leading authority on quality. With more than 90,000 individual and organizational members, the not-for-profit professional association advances learning, quality improvement and knowledge exchange to improve business results, and to create better workplaces and communities worldwide. As champion of the quality movement, ASQ offers technologies, concepts, tools and training to quality professionals, quality practitioners and everyday consumers, encouraging all to Make Good Great®. ASQ has been the sole administrator of the prestigious Malcolm Baldrige National Quality Award since 1991. Headquartered in Milwaukee, Wis., the 60-year-old organization is a founding partner of the American Customer Satisfaction Index (ACSI), a prominent quarterly economic indicator, and also produces the Quarterly Quality Report.



To: The Securities and Exchange Commission

Re: SEC File No. S7-24-06

Subject: The American Society for Quality Sarbanes-Oxley Team Comments on “Management’s Report on Internal Control over Financial Reporting”

1.0 Introduction

The SEC is proposing *Management’s Report on Internal Control over Financial Reporting* which provides interpretive guidance for management regarding its evaluation of internal control over financial reporting. The proposed guidance is intended to assist companies of all sizes to complete their annual evaluation in an effective and efficient manner.

The SEC requested the following types of comments on the document:

- **Clarification.** Are there particular areas within the proposed interpretive guidance where further clarification is needed? If yes, what clarification is necessary?
- **Aspects not addressed.** Are there aspects of management’s annual evaluation process that have not been addressed by the proposed interpretive guidance that commenters believe should be addressed by the Commission? If so, what are those areas and what type of guidance would be beneficial?

The SEC has invited interested parties to comment on the document. The Sarbanes-Oxley (SOX) Team consisting of five members of the American Society for Quality (ASQ) SOX Community¹ was asked to comment on the interpretative guidance. Over the past two years, the “Team” has conducted 2 ASQ SOX conferences, a webinar and 6 workshops and presented numerous papers at conferences and in publications such as

¹ The five members are Dr. Sandford Liebesman, ASQ Fellow and Chairman-Elect ASQ Electronics and Communications Division, Paul Palmes, Vice-Chairman US Technical Advisory Group to ISO TC 176 (the developer of ISO 9001), John Walz, The Sutton Group, Donna Spencer, The NORDAM Group and Marty Jaeger, Jaeger-Holland.

ASQ's *Quality Progress* and The Institute of Internal Auditors (IIA) publication the *Internal Auditor*.

The Team has shown that the quality and environmental management systems (QMS/EMS) of public companies can directly support SOX compliance. Many public companies are registered to the QMS standard ISO 9001:2000² and the EMS standard ISO 14001:2004³. We will show how satisfying these standards provides valuable inputs to the management reporting process.

A member of the Team published articles in the September 2005 issue of *Quality Progress*⁴ and the October 2005 issue of the *Internal Auditor*⁵ linking these ISO standards to Internal Controls – Integrated Framework by COSO, the most common system used to comply with the Sarbanes-Oxley (SOX) Section 404 requirement to have an effective system of internal control. The Team wishes to point out how robust management systems, using these two ISO standards, can be extended to support the financial management systems compliance efforts.

The comments below describe specific parts of the proposed management guidance where QMS/EMS support applies. The comments focus on the strengths that quality and environmental management bring to the table: clarification of management's roles and responsibilities, methodology for the control of documents and data as guidance to information technology management, support of COSO guidance, monitoring and measurement of processes and products, definition of the Organization's measurable objectives, identification of risks to these objectives, definition of preventive and corrective action tools to manage risks, and valuable risk indicators that can be obtained from a review of records required by the two ISO standards.

² ISO 9001:2000 Quality Management System Requirements As of December 2005, the number of ISO 9001 registrations was 776,608 worldwide, 59,663 in North America and 44,270 in the United States. Registered organizations are audited every six months by an accredited registrar. The United States accreditation agency is the RABQSA.

³ ISO 14001:2004 Environmental Management System Requirements. As of December 2005, the number of ISO 14001 registrations was 56,593 worldwide, 7,119 in North America and 5,061 in the United States. Registered organizations are audited every six months by an accredited registrar. The United States accreditation agency is the RABQSA.

⁴ Sanford Liebesman, "Mitigate SOX Risk with ISO 9001 and 14001," *Standards Outlook, Quality Progress*, September 2005, 91-93.

⁵ Sanford Liebesman, "Quality in the Mix," *Risk Watch Column, The Internal Auditor*, October 2005, 73-77.

2.0 Comments on “Management’s Report on Internal Control over Financial Reporting”

Comment #1: page 12: footnote. “The term “entity-level controls” as used in this document describes aspects of a system of internal control that have a pervasive effect on the entity’s system of internal control such as controls related to the control environment (e.g., **management’s philosophy and operating style, ... assessment of authority and responsibility, ...**) ... the company's risk assessment process; centralized processing and controls, including shared service environments; controls to **monitor results of operations.**”

QMS/EMS Comment: Clarification: Some of the means by which this may be accomplished may be found in various clauses of ISO 9001 and ISO 14001.

- **QMS:** Assessment of authority and responsibility is defined in ISO 9001, Clause 5.5, Responsibility, Authority and Communication; and **EMS:** ISO 14001, Clauses 4.4.1 and 4.4.3, Resources, Roles, Responsibilities, Authority and Communication.
- **QMS:** Controls to monitor results of operations are described in ISO 9001, Clauses 8.2.3 and 8.2.4, Monitoring and Measurement of Product and Processes; and **EMS:** ISO 14001, 4.5.1, Monitoring and Measurement.

Comment #2: page 14: “Management should use its own experience and informed judgment in designing an evaluation process that aligns with the operations, financial reporting risks and processes of the company.”

QMS/EMS Comment: Clarification:

- **QMS:** ISO 9001, Clauses 5.6 Management review, 8.2.2 Internal audit, and 8.4 Analysis of data align Operational compliance evaluations to Financial evaluations.
- **EMS:** ISO 14001, Clauses 4.6 Management review, 4.5.5 Internal audit, and 4.5.2 Evaluation of compliance align Operational compliance evaluations to Financial evaluations.

Comment # 3: pages 18 and 19: “A. 1. d. Role of General Information Technology Controls.”

QMS/EMS Comment: Clarification:

- **QMS:** ISO 9001, Clauses 4.2.3 and 4.2.4 require documented procedures for the control of documents and records.
- **EMS:** ISO 14001, Clauses 4.4.5 and 4.5.4 require procedures for the control of documents and records.

Comment # 4: page 20 Footnote: “For example, both the COSO framework and the Turnbull Report state that determining whether a system of internal control is effective is a subjective judgment resulting from an assessment of whether the five components (i.e., control environment, risk assessment, control activities, monitoring, and information and communication) are present and functioning effectively.”

- **QMS/EMS Comment: Aspects not addressed:** ISO 9001 and ISO 14001 provide support for the COSO guidance as described in Table 1: Comparison: COSO Components and ISO 9001/14001 Requirements in the paper “Mitigate SOX Risk with ISO 9001 and 14001” by Sanford Liebesman (see footnote 4).

Comment # 5: page 22: “a. Identifying Financial Reporting Risks: Ordinarily, the identification of financial reporting risks begins with evaluating how the requirements of GAAP apply to the company’s business, operations and transactions.”

QMS/EMS Comments: Aspects not addressed:

- **QMS:** ISO 9001, Clauses 5.3 Quality policy, 5.4 Planning, and 8.5.3 Preventive action start the Operational Risk Management activities that will impact financial risks.

Comment # 6: page 22 Footnote: “Monitoring activities are those that assess the quality of internal control performance over time. These activities involve assessing the design and operation of controls on a timely basis and taking necessary corrective actions. This process is accomplished through on-going monitoring activities, separate evaluations by internal audit or personnel performing similar functions, or a combination of the two. On-going monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory review activities”.

QMS/EMS Comments: Aspects not addressed:

- **QMS:** ISO 9001, Clause 8.2.3 requires “Monitoring and measurement of [the organization’s] processes” and Clause 8.4 requires analysis of data obtained as a result of Clause 8.2.3. The results of the analysis are used in the identification of risks to the organization’s objectives and provide inputs to the corrective and preventive action processes (Clauses 8.5.2 and 8.5.3).
- **EMS:** ISO 14001, Clause 4.5.1 requires monitoring and measurement, on a regular basis, of the key characteristics of its operations that can have a significant environmental impact and Clause 4.5.2 requires evaluation of compliance
- **QMS/EMS:** Regular management reviews are addressed in ISO 9001, Clause 5.6 and ISO 14001, Clause 4.6.

Comment # 7: page 23: “Management uses its knowledge and understanding of the business, its organization, operations, and processes to consider the sources and potential likelihood of misstatements in financial reporting elements and identifies those that could result in a material misstatement to the financial statements (“financial reporting risks”).”

QMS/EMS Comments: Aspects not addressed: Many financial reporting risks can be sourced to Operational risks. To avoid redundant processes and expenses, Management can combine or integrate appropriate operational and financial activities.

- **QMS:** ISO 9001, Clauses 5.3 Quality policy, 5.4 Planning, and 8.5.3 Preventive action starts the Operational Risk Management activities that will impact financial risks.

Comment # 8: page 24 Footnote. “Controls within a process may consist of financial reporting controls and operational controls (i.e., those designed to achieve operational objectives).”

QMS/EMS Comments: Clarification:

- **QMS:** ISO 9001, Clauses 5.4.1, Quality Objectives, 5.4 Planning, 8.2 Monitoring and measurement, and 5.6 Management review requires a definition of measurable objectives at relevant functions and levels within the organization, which are planned, managed, measured, and reviewed by management
- **EMS:** ISO 14001, Clause 4.3.3, Objectives, Targets and Programme(s) requires measurable environmental objectives and targets.

Comment # 9 page 25 Footnote. “Preventive controls have the objective of preventing the occurrence of errors or fraud that could result in a misstatement of the financial statements. Detective controls have the objective of detecting errors or fraud that has already occurred that could result in a misstatement of the financial statements. Preventive and detective controls may be completely manual, involve some degree of computer automation, or be completely automated.”

QMS/EMS Comments: Aspects not addressed:

- **QMS:** ISO 9001, Clauses 8.5.2 Corrective action and 8.5.3 Preventive action provide best practices for addressing actual and potential risks and their prevention or correction.
- **EMS:** ISO 14001, Clause 4.5.3 provide best practices for dealing with actual and potential risks and for taking corrective or preventive actions.

Comment # 10: pages 26 and 27 Footnote. “Controls that are designed to have a specific effect on a financial reporting element are considered directly related. For example, controls established to ensure that personnel are properly counting and recording the annual physical inventory relate directly to the existence of the inventory.”

QMS/EMS Comments: Aspects not addressed:

- **QMS/EMS:** Inventory management is a normal activity of the Quality Management System. Valuable inputs can be provided by a review of the operations of the organization and records required by ISO 9001 and ISO 14001. This is true of all activities of an organization.

Comment # 11: page 28: “While general IT controls ordinarily do not directly prevent or detect material misstatements in the financial statements, the proper and consistent operation of automated or IT dependent controls depends upon effective general IT controls.”

QMS/EMS Comments: Aspects not addressed: IT design principles require mapping of information from its source to its outputs; when these outputs are financial, then design of IT controls starts at the source, most likely in Operations.

- **QMS:** ISO 9001, Clauses 7.1 Planning of product realization, 7.3 Design and development, 7.6 Control of monitoring and measuring devices. and 8.2.3 Monitoring and measurement of processes guide IT Control design alignment with both Operations and Financial activities.

Comment # 12: pages 28: “Documentation of the design of the controls management has placed in operation to adequately address the financial reporting risks is an integral part of the reasonable support. The form and extent of the documentation will vary depending on the size, nature, and complexity of the company.”

QMS/EMS Comments: Aspects not addressed: Documentation of the design of the controls and records for control operations are defined in the QMS.

- **QMS:** ISO 9001, Clauses 4.2 Documentation requirements covers both control design documentation and records showing control of operations.

Comment # 13: page 35. “Evidence that is relevant to the assessment may come from activities that are performed for other reasons (e.g., day-to-day activities to manage the operations of the business).” and **page 35 Footnote:** “Many commenters on the Concept Release requested guidance clarifying that evidence relevant to supporting the evaluation may come from activities that are integrated into management’s daily activities or performed for other reasons.”

QMS/EMS Comments: Clarification:

- **QMS/EMS:** Valuable inputs can be provided by a review of the operations of the organization and records required by ISO 9001 and ISO 14001.

Comment # 14: pages 46 and 47. The Commission’s rule implementing Section 404 was intended to bring information about material weaknesses in ICFR into public view. Because of the significance of the disclosure requirements surrounding material weaknesses beyond specifically stating that the material weaknesses exist, companies should also consider including the following in their disclosures: the nature of any material weakness and management’s current plans, if any, for remediating the weakness.”

QMS/EMS Comments: Aspects not addressed:

- **QMS:** ISO 9001, Clauses 8.5.2, Corrective Action and 8.5.3, Preventive Action, document remediation procedures that are available to management.
- **EMS:** ISO 14001, Clause 4.5.3, Nonconformity, Corrective Action and Preventive Action, documents remediation procedures that are available to management.

4.0 Conclusions

Quality and environmental management systems provide support for compliance to the Sarbanes-Oxley Act. Organizations that comply with Quality Management System Standard ISO 9001 and the Environmental Management System Standard ISO 14001 have demonstrated the existence of processes and procedures that can support top management in their compliance efforts and increase the information available to auditors during the attestation process.

The American Society for Quality is the largest quality organization in the world. The observations and recommendations in this letter are meant to have broad application in the public and private sectors throughout the world. Quality and environmental management systems provide valuable inputs to an organization's financial structure that help maintain its competitiveness in the global economy. The ASQ SOX Team will be pleased to provide further details on the comments in this letter.

Respectfully submitted,



Dr. Burton S. Liebesman, Ph.D.
Chairman-Elect
ASQ Electronics and Communications Division

February 23, 2007