THE INFORMED OUTLOOK®

...your source for the latest information on international management system standards

SPECIAL REPRINT

SOX Stimulates Continual Improvement

The Impact of SOX and QMS/EMS on Corporate Governance

By Sandford Liebesman, Paul Palmes and John Walz

Publisher's Note: This article has been reprinted with permission from THE INFORMED OUTLOOK *Newsletter, April 2004 issue.*

The Sarbanes-Oxley Act of 2002 (SOX) shares one overriding goal with ISO 9001 and ISO 14001: continual improvement of organizational effectiveness. Indeed, we have found that the most important reaction to SOX is to stimulate an improvement in the governance of public corporations by virtue of its requirements that a company's Top Management—in this case, the Chief Executive Officer (CEO) and Chief Financial Officer (CFO)—certify the appropriateness of each financial statement released by the company.

To conform to the financial reporting requirements of SOX, a corporation must ensure its financial management processes, including its internal controls, are effective and will improve over time. This is similar to what is required in terms of continual improvement of the effectiveness of a quality management system (QMS) for conformity with ISO 9001:2000 and of an environmental management system (EMS) with ISO 14001. Thus, the requirements in all three cases seek improvement in corporate governance. In ISO 9001 and ISO 14001 terms, this is known as Management Commitment, which includes quality and environmental policies and objectives, internal communication and Management Review.

In earlier articles in this series, we have examined the sections of SOX that relate to Top Management's responsibilities and obligations, introduced the concept that there is a linkage between the procedures required to comply with SOX and those contained in QMSs and EMSs conforming with ISO 9001 and ISO 14001 and explored how the linkage can strengthen the internal controls and auditing process and reduce the risks faced by public companies. In the most recent article, we showed how one company, Otter Tail, was using its QMS to support compliance with SOX and reduce corporate risk.

The question now is: What impact does SOX have on the broader issue of corporate governance? A corollary question is: What roles can the management systems and internal auditors play in ensuring that the internal controls will prove effective when external auditors evaluate those controls? The reality is that compliance with the external auditing of internal controls is required. So, the key opportunity is in turning compliance into an opportunity for cost-effective organizational improvement. What's more, growing interest in SOX outside the United States means that real conformity with international management system standards may be the way to ensure global conformity with government regulations and, as a by-product, improve the effectiveness of global management systems.

The fact is that QMSs and EMSs provide tools to support the system of internal controls and help internal auditors develop their reports to Top Management and the Board of Directors (BOD). We will conclude this series of articles with a look at the subject as one of global importance.

Are You Ready for Third-Party Audits of Internal Controls?

Internal controls are designed to assure the achievement of objectives and goals, especially in regards to the effectiveness and efficiency of processes, the reliability of financial reports and the organization's compliance with applicable laws and regulations.

On March 9, 2004, the Public Company Accounting Oversight Board (PCAOB) unanimously adopted Auditing Standard No. 2 and sent it out for comment by April 23, 2004. [Note: Public comment is due April 23, 2004. Written comments should be sent to the Office of the Secretary, PCAOB, 1666 K Street, NW, Washington, DC 20006-2803. Comments may also be submitted by e-mail (comments@pcaobus.org) or through the PCAOB's web site (www.pcaobus.org).]

Auditing Standard No. 2 contains a requirement that the external auditors of financial statements must also conduct annual audits of a public company's internal controls. SOX requires that the CEO and CFO will report on the effectiveness of internal controls and that auditors have to vouch for the accuracy of Top Management's statements. The PCAOB standard explains the SOX auditing requirements. While the requirement will not become binding on public companies unless the Securities and Exchange Commission (SEC) approves

Standard No. 2, the proposed effective date is November 15, 2004.

As noted in the first and second articles in this series, SOX authorized the creation of the PCAOB to prescribe a control model and auditing procedures. The PCAOB has endorsed the model developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. COSO includes the following five requirements for internal controls, which are part of PCAOB's Auditing Standard No. 2:

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring.

It is expected that financial accounting firms will have more responsibility and work as a result of the requirements adopted by the PCAOB. However, if the SEC approves it, it would mean that effective management of all systems—including the QMS and/or EMS—will be critical to support compliance with SOX. In effect, the PCAOB standard requires that Top Management demonstrate true commitment to the management systems, which will in turn ensure full compliance with SOX.

The new PCAOB framework identifies three primary objectives of internal control: efficiency and effectiveness of operations; financial reporting; and compliance with laws and regulations. These were also the COSO objectives.

Not all controls relevant to financial reporting are accounting controls. Accordingly, controls that could materially affect financial reporting include controls that focus on the effectiveness and efficiency of operations or compliance with laws and regulations. These will have a material effect on the reliability of financial reporting and are a part of internal control.

"The standard adopted yesterday calls for outside auditors to do more than take management's word," wrote David S. Hilzenrath in "Proposal Asks for Audits of Firms' Internal Checks" in the March 10, 2004, issue of *The Washington Post*. As described by Hilzenrath, these third-party audits by the financial auditors sound very much like what should be occurring in the auditing of a process-based QMS or EMS. "They would be required to conduct annual 'walkthroughs,' tracing sample transactions through a company's system until they are reflected in the financial statements. The standard also requires auditors to assess the effectiveness of boards of directors' audit committees.

"The standard requires auditors to disclose whether a company had 'material weaknesses' in internal controls at the end of the fiscal year. If a company corrected serious breakdowns by the end of the year, the public would not necessarily be informed." However, Douglas R. Carmichael, the PCAOB's Chief Auditor, was reported to have indicated that, even if corrected, these "material weaknesses" would likely be disclosed.

The need for external audits of the internal controls will raise the cost of SOX compliance, but that cost may be minimized—as would the risk of a nonconformity involving the controls—if a public company had effective management systems. With the direct involvement of Top Management in those systems and a clear message from management that all employees must follow established management system processes and procedures, the organization would be vigilant in maintaining and improving its processes and system elements. This will include the internal controls in the financial management system. And if the company were to include the financial operations in the scope of the QMS and/or EMS, combined quality, environmental and financial internal audits will help ensure that the internal controls remained effective and efficient.

Corporate Governance in a Systems and SOX Environment

One of the great challenges, as noted throughout this series of articles, is for those responsible for ISO 9001 and/or ISO 14001 conformity to communicate with Top Management in terms that Top Management understands and considers important to the business. But the real opportunity for the QMS and EMS managers is in showing how the systems can help meet the key objective of SOX, which is to improve corporate governance so that financial statements represent a true report of the state of the corporation. Because SOX is a regulatory requirement for public companies in the United States and may become a model for requirements adopted in other countries in the future, SOX is something that ISO 9001 and ISO 14001 require a company to consider and comply with, and linking ISO 9001 and ISO 14001 to legislation similar to SOX is a global issue.

A public company that has a QMS and/or EMS should be structured much like the governments of democratic countries, with a separation of powers. There are four powers or constituencies within a public company:

1. The CEO
2. Various levels of management
3. The employees
4. The BOD.

Each of the four has its own roles and responsibilities. The CEO is responsible for the operation of the business, with support from the various levels of management in carrying out the corporate goals and managing the employees who carry out the functions of the organization. Overseeing all of this and providing corporate governance is the BOD.

In a presentation titled "Quality Assessments for Improvement in Corporate Governance" at the 2003 Annual

Reprinted with permission from
THE INFORMED OUTLOOK
April 2004 issues

INFORM ✧ 6 Arrowwood Court, Durham, North Carolina 27712
Tel: 1-877-463-6769 (toll free) or 919-479-6939 ✧ Fax: 919-471-6413
E-Mail: JIM@INFORMINTL.COM ✧ Web Site: HTTP: WWW.INFORMINTL.COM

Quality Congress (AQC), Tito Conti, Managing Partner of Organizational Assessment Management in Ivrea, Italy, stated that good governance involves the logical functions of the business: (a) strategic guidance; (b) global oversight; (c) company management; and (d) monitoring and assessment. Conti noted that the responsibilities of the organization are well-defined in the Principles of Corporate Governance of the Organization for Economic Co-operation and Development (OECD):

- Protecting the rights of the shareholders
- Ensuring equitable treatment of all shareholders
- Recognizing the rights of all stakeholders
- Having the BOD, as part of its responsibilities, provide strategic guidance, effective monitoring and accountability
- Ensuring timely and accurate disclosure and transparency.

Indeed, the BOD is supposed to represent the shareholders by assessing the state of the organization and taking appropriate actions when necessary. Unfortunately, this is not the case in some public companies, where the Board is often not independent of the CEO and of other members of Top Management. Such boards are not considered to be operating in a "professional" manner, not to mention the fact that they raise the risk of not complying with SOX.

In a presentation titled "The Impact of Corporate Governance in the Quality of Management" at the 2003 AQC, Dr. Marcos E. J. Bertin, Chairman of the Board of the International Academy for Quality (IAQ), raised the following points about professional BODs:

- Research by the National Association for Corporate Directors indicated that companies with professional BODs generate 1.5-2.0% more value for their shareholders that traditional boards.
- In addition, investment funds pay up to 28% more for the shares of companies that organize their work in keeping with the best practices recommended by these institutions.

Bertin related that a team of experts from the IAQ was chartered to produce criteria to evaluate the quality of BODs. The criteria will be built upon the following four core values to be embodied by BODs:

1. Leadership, independence, ethics and transparency
2. Understanding of the difference between Governance and Management
3. A focus on well-documented processes that add value
4. A focus on continual improvement.

Upon examination, these values will also be found to be embedded in any effective QMS or EMS. While the goal of an effective QMS or EMS is Management Commitment and performance improvement driven by Top Management, the end result is effective and profitable corporate governance.

Quality, Risk and the BOD

The fact is that quality is a subject for the BOD of any public company to understand and in which to place value. The national and international quality awards—the Malcolm Baldrige National Quality Award (MBNQA), European Foundation for Quality Management (EFQM) award and Deming Prize are among the most well-known—involve assessment of organizations against criteria and propose core values that form models for competitiveness and guidance for BODs. Likewise, ISO 9001:2000 and ISO 14001:1996 provide a methodology for process management that is essential to good governance.

For example, professional boards will follow the quality improvement process built around the plan➜do➜check➜act (PDCA) cycle, as follows:

- Plan—Deploy the Quality Policy and objectives
- Do—Implement the Policy and achieve the objectives
- Check—Review the Policy to ensure it is being adhered to and pursued, with the use of the results from
  - Quality/Internal audits
  - Risk assessments
- Act—Revise the Policy as needed.

In his presentation titled "Corporate Governance: Quality at the Top" at the 2003 AQC, Gregory H. Watson, Managing Partner of Business Systems Solutions International, Inc., stated that the BOD should consider three types of risk:

1. "Producer's risk", which occurs when the organization makes promises to its stakeholders it can't keep. For example, issuing revenue projections that are unrealistic and promised cost reductions that are not met.
2. "Consumer's risk", which occurs when the organization does not design product/services to meet the expectations of its customers. For example, major customers that are depending on the organization's new designs that then fail to meet the customers' needs. Other examples are recalls, high failure rates, safety/environmental issues and lower than expected ramp-up.
3. "Shareholder's risk", which occurs when the other risks take place simultaneously, resulting in the company's products or services not being competitive.

A good example of these risks occurred in the telecommunications industry during the bubble of 2000, when companies in the telecom sector were projecting revenues at unrealistic levels and the overextension of the sector's resources failed to take into consideration customer needs.

In his presentation, Conti defined a framework for corporate governance related to a new way of applying QMS assessments. He suggested that companies can apply four types of internal assessments:

1. Company self-assessment—a combination of an internal financial audit and a quality assessment, where a company reviews its current goals, the previous year's results, the performance achieved by its competitors and future goals.
2. CEO self-assessment—that is, this is the CEO's evaluation of how well his or her expectations were met.
3. CEO assessment by the BOD's Compensation Committee—this assessment looks at the company's financial performance as well as its level of customer satisfaction and its long-term success.
4. BOD self-assessment—the aim of this self-assessment is to determine what can be done to improve corporate governance, and it provides visibility for the stakeholders.

Three goals of corporate governance are management of risk, effective process management and continual improvement of company performance. The internal controls for the

financial "management system" are linked to these three, particularly effective process management. QMSs and EMSs in conformity with the requirements of standards such as ISO 9001:2000 and ISO 14001:1996 are excellent tools for accomplishing the BOD's objectives, including those set to meet these goals.

Change the Culture to Prevention Instead of Correction

However, the BOD needs to move the corporate mentality from correcting problems to preventing them. Accomplishing these goals of prevention will provide an excellent step toward satisfying the requirements of the Sarbanes-Oxley Act of 2002 and will lead to continual corporate improvement. QMS and EMS practitioners can help satisfy the SOX requirement through effective system maintenance and use throughout the organization, including the application of the eight quality management principles.

In his keynote address at the 2003 AQC, Horst Schulze, former President and CEO of the Ritz Carlton Hotels, a two-time Baldrige winner, talked about key quality principles. These include Top Management leadership, customer focus, process management, preventive action, continual improvement, objectives and valuing employees. But Schulze's most telling comment was that "quality practitioners have a moral obligation to teach quality to Top Management. What creates money in the long-term is the excellence of the company." This is an excellent point to keep in mind when considering efforts at continual improvement of your organization's management system, particularly if the company is subject to SOX. ###

[Editor's Note: A team was recently formed to develop an understanding of the relationship between financial and quality and environmental auditing processes and to alert quality and environmental practitioners to the opportunities for providing inputs to Top Management and the Boards of Directors in their organizations. All members of the team contributed to this article.]

The team is called the SOX_Q/E Management Team whose members are:
***Sandford Liebesman**, PhD, Principal of Sandford Quality Consulting, LLC, who can be contacted by e-mail (sandfordl@msn.com).*
***Lawrence Liebesman**, Partner, Environmental Practice, Holland & Knight LLP, who can be contacted by e-mail (lliebesman@hklaw.com).*
***Paul Palmes**, Quality Assurance Director, Northern Pipe Products Inc., who can be contacted by e-mail (paulp@northernpipe.com).*
***John Walz**, Quality Management System Consultant, who can be contacted by e-mail (johnwalz@ameritech.net).*

