THE INFORMED OUTLOOK®

January 2004 ✧ Volume 9, Number 1

...THE EVOLUTION AND USES OF MANAGEMENT SYSTEM STANDARDS: ISO 9000, ISO 14000, ET AL

Inside THE OUTLOOK

Can a QMS/EMS Help You Deal With the Sarbanes-Oxley Act?

Use Management Tools to Mitigate Risk From SOX

By Sandford Liebesman

What is the biggest concern for Top Management in US companies today? It is risk, which *The American Heritage Dictionary of the English Language* (Houghton Mifflin Co., 1981) defines as "suffering harm or loss; danger; hazard; a factor, element or course involving uncertain danger".

In today's business environment, Top Management's greatest concerns are forms of risk other than the danger of a terrorist attack—financial risk, competitive risk and the newest risk, the Sarbanes-Oxley Act of 2002 (SOX). What is SOX and how does it affect the management of public companies? According to this Act of Congress, the Chief Executive Officer (CEO) and

(page 12, SARBANES-OXLEY)

KEY POINTS

TOP MANAGEMENT'S GREATEST CONCERNS ARE FINANCIAL RISK, COMPETITIVE RISK AND THE NEWEST RISK, THE SARBANES-OXLEY ACT OF 2002

SOX REQUIRES THAT THE CEO AND CFO OF A PUBLIC COMPANY IN THE US NOW HAVE TO CERTIFY THE APPROPRIATENESS OF EACH FINANCIAL STATEMENT THAT THEIR COMPANY RELEASES

THERE IS NOTHING TO PREVENT AN ORGANIZATION FROM USING ITS MANAGEMENT SYSTEM(S) TO ADDRESS RISK

TO COMPLY WITH SOX, A COMPANY IS REQUIRED TO INVESTIGATE OPERATIONS WITHIN THE ORGANIZATION—FINANCIAL AUDITS—TO ENSURE THAT ITS WORKING SYSTEMS SUPPORT THE NUMBERS IN THOSE FINANCIAL STATEMENTS

THE OBVIOUS SYNERGY BETWEEN SOX AND THE ISO 9001:2000 AND ISO 14001:1996 STANDARDS HAS LARGELY GONE UNNOTICED AND UNEXPLORED BY PUBLIC COMPANIES IN THE US

MANY TOP MANAGERS DO NOT REALLY UNDERSTAND THE NATURE OF A QMS OR EMS AND HOW SUCH SYSTEMS CAN BE HARNESSED TO ENSURE FINANCIAL MANAGEMENT COMPLIES WITH SOX

FOUR KEY ASPECTS ARE MANDATED BY SOX FOR A PUBLIC COMPANY THAT STRONGLY AFFECT THE MANAGEMENT OF ALL ORGANIZATIONS:

1. INTERNAL CONTROLS
2. CORPORATE RECORDS
3. INTERNAL FINANCIAL AUDIT FUNCTION
4. THE AUDIT COMMITTEE

THE PRIMARY FILTER AND CONCERN FOR TOP MANAGEMENT IS NOW RISK

Use Management Tools to Mitigate Risk From SOX

(from front page — SARBANES-OXLEY)

Chief Financial Officer (CFO) of a public company in the United States now have to certify the appropriateness of each financial statement that company releases. Failure may mean civil suits or even jail time.

Enron and WorldCom shared a common disconnect between what was reported and actual practice. Financial audits had the potential to prevent these scandalous outcomes, but instead they were being misused to hide problems. Financial audits have been required of public (and most other) companies for quite some time, and they provide background information to help decision-makers better manage company resources and direct attention to profitable improvement efforts. However, these same audits are integral to financial management reporting and they should be conducted in a way that provides shareholders with a degree of safety and reassurance about a given company at the operating level.

There is nothing to prevent an organization from using its management system(s) to address risk through the development and application of procedures as part of its system(s). After all, to comply with SOX, a company is required to investigate operations within the organization—financial audits—to ensure that its working systems support the numbers in those financial statements. And SOX requires the CEO and CFO—key members of the Top Management of any public company—to certify the appropriateness of financial statements. So, how does a public company pursue and maintain compliance with SOX? And what can a quality management system (QMS) and/or environmental management system (EMS) do to contribute to that compliance?

ISO 9001:2000 and ISO 14001:1996 share common requirements concerning the auditing, review and continual improvement of the QMS/EMS—including the adherence to regulations and the demonstrated existence of principled Top Management involvement (ISO 9001:2000 uses the term "management commitment"). The Sarbanes-Oxley legislation is designed to accomplish much the same things and, in the process, to restore investor confidence in the marketplace. The unfortunate truth is that the obvious synergy between this legislation and the two ISO standards has largely gone unnoticed and unexplored by public companies in the United States. And many of these companies are registered to the two standards and have available to them valuable data and information gathered by their management systems.

This situation may be the result of a seeming contradiction of sorts. The linkage may be too difficult for members of Top Management to see because, while they are paying a great deal of attention to SOX and what it takes to comply with the law. Many Top Managers do not really understand the nature of a QMS or EMS and how such systems can be harnessed to ensure financial management complies with SOX. At the same time, perhaps the linkage is simply too obvious to the individuals within the organization who deal with the QMS and/or EMS every day. They assume Top Management sees the linkage as well or they don't know how to communicate—and act on—the potential value to those responsible for compliance with Sarbanes-Oxley.

Within the walls of any ISO 9001- or ISO 14001-conforming organization, registered or not, personnel are routinely engaged in system and process auditing. Such activities are routine, an accepted part of the QMS or EMS. And the routine is well-known: audits are conducted, audit findings are reported, corrective actions are engaged in to address the nonconformities found and verification of the effectiveness of the corrective actions follows. Each of these

(next page, SARBANES-OXLEY)

SARBANES-OXLEY

(from previous page)

activities is an indication of sound operational practice and control. In addition, measured inputs and outputs, established criteria, employee competency, process planning and solid design practices are expected outcomes of the processes that make up the management system. Unfortunately, the operational nature and terminology of an ISO 9001-conforming QMS or ISO 14001-conforming EMS—and the profile of concerns that audits of these systems raise—fly below the radar of Top Management in many organizations and fail to show up in many executive boardroom discussions.

Instead, the boardroom relies on the financial statements to decide where and how to allocate resources to manage the organization and its operations (and future growth). And as "the financials" are built upon and reflect the success or failure of operations, further involvement in direct management of the organization—especially operational oversight—is often delegated to others within the company. The logical outcome is a disconnect between operational reality and Top Management resource planning and control. In other words, the typical scenario deprives Top Management of the very resource, the management system, that could ensure the financials are accurate and lead to effective decisions and operational improvement.

In "Manager's Journal," in *The Wall Street Journal* on June 24, 2003, Samuel A. DiPiazza, CEO of PriceWaterhouseCoopers, and Dennis M. Nally, Chairman and Senior Partner of the US member firm, suggested the need for "a new and higher standard of corporate disclosure. That standard would oblige companies to report externally the information—financial and non-financial, historical and perspective—that they use internally to manage their business."

The likelihood is that the Sarbanes-Oxley legislation will cause a change in the reporting process. The legislation specifically calls for quality control of not only the financial reports, but also the processes and systems that combine to provide input to those reports. This makes a clear case for using ISO 9001 and/or ISO 14001 conformity in a way not anticipated when these standards were developed.

In addition, the case has been made for the quality and environmental management inputs having an effect on the compensation given to executives. In a July 30, 2003, interview on National Public Radio's "All Things Considered" with Robert Siegel, William Donaldson, Chairman of the Securities and Exchange Commission (SEC), noted that "the compensation committees must look at real performance in addition to financial measures. These include product quality, customer satisfaction and investment in research."

Using ISO 9001/ISO 14001 management systems to comply with SOX's requirements is therefore not only a compelling opportunity to add value to these systems, but it is also a cost-effective approach. The quality and environmental auditors of a public company having a QMS and an EMS are already looking in the right places to satisfy both the standard(s) and the legislation.

Compared with a decade ago, when the 1994 editions of ISO 9001/2/3 were nearing completion and most organizations using QMSs now did not have formal systems, today's quality professional is increasingly expected—or should be expected—to assume the role of an active and cost-effective participant in business planning and risk management. I cannot think of a better way to transition the role of a company's "Quality Department" from providing occasional inputs to becoming the permanent oversight of system effectiveness.

The same holds true for environmental professionals, although a much smaller number of US organizations today have EMSs registered to ISO 14001 (3,197 certificates as of January 20, 2004, vs. more than 40,000 for ISO 9001:2000), and there are likely proportionately fewer in conformity without registration than on the QMS side of the equation. However, using both standards to manage financial risk is the best approach to accurate reporting. Combining elements of the management systems required by ISO 9001 and ISO 14001 with procedures for compliance with SOX can ensure effective compliance while using existing resources. From financial and management system standpoints, this is a highly desirable outcome.

After all, conforming to ISO 9001 and ISO 14001 requires an organization to have a highly trained and competent staff to maintain and continually improve the QMS and EMS or an integrated management system (IMS). These personnel are perfectly prepared and positioned to support the Sarbanes-Oxley "quality control" audit function. And, in the spirit of ISO 9001 and ISO 14001, Top Management is the beneficiary of information gathered relative to the management system(s) that is vital to responsible control, resource management and accurate, effective reporting. Thus, many public companies have the opportunity to achieve compliance with SOX and simultaneously strengthen their ISO 9001- and ISO 14001-conforming QMSs and EMSs.

It will help you to see where and how your company's QMS and/or EMS can help achieve and maintain compliance with SOX by taking a look at this piece of legislation.

The Sarbanes-Oxley Act

In their June 24, 2003, column in *The Wall Street Journal*, DiPiazza and Nally declared that, in the past, "[some] publicly traded companies issued misleading financial statements at the direction of senior executives and sometimes with the assistance of outside auditors." Indeed, the Sarbanes-Oxley legislation, which was passed by Congress and signed into law in August 2002, was enacted largely in response to the financial and accounting scandals at US

(next page, SARBANES-OXLEY)

SARBANES-OXLEY

(from page 32)

corporations such as Enron and WorldCom. (The Italian conglomerate Parmalat is now the subject of an investigation concerning a financial scandal, which demonstrates that companies in other countries are not immune from such events and might therefore also want to use their QMSs and EMSs to ensure financial statements are accurate.)

In an October 2002 article in *Quality Digest* titled "Value-added Auditing: Your Best Assessment Tool", Greg Hutchins, a Management Principal with Quality Plus Engineering in Portland, OR, wrote that Steve Jameson, Director of Technical Services at the Institute of Internal Auditors, made the following statement in 2002:

> *Requiring public reporting on internal controls has been the grand prize that the internal auditing profession has sought for years. The US Congress has now mandated that requirement.*

But what does the actual requirement mean for a public company and what is the intended result of the legislation? First introduced in the US House of Representatives on February 14, 2002, and signed by President Bush on July 30, 2002, as Public Law Number 107-204, its official "title" is:

> *An Act*
> *To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.*

What follows is a look at the key imperatives of SOX, as found in five sections of this Act of Congress. The text of these five sections can be found in sidebars on or near the pages where each is discussed.

Section 103: Auditing, Quality Control, and Independence Standards and Rules

The sidebar on the next two pages that contains Section 103 also provides four of the definitions contained in the Sarbanes-Oxley Act of 2002. I have included these because they define terms that are relevant to management systems but where the definitions for SOX are in some cases different.

SOX authorized the creation of the Public Company Accounting Oversight Board (PCAOB), which is referred to in Section 103 and elsewhere in SOX as the "Board". Section 103 addresses the need to select and/or establish auditing, quality control and ethics standards and rules to be used by registered public accounting firms in auditing public companies and issuing accounting reports. The American Institute of Certified Public Accountants (AICPA) has evaluated SOX and posted a summary of the Act on its web site (www.aicpa.org). In its summary of Section 103, the AICPA indicates that the PCAOB shall take the following 7 actions:

1. register public accounting firms;
2. establish, or adopt, by rule, "auditing, quality control, ethics; independence, and other standards relating to the preparation of audit reports for issuers;"
3. conduct inspections of accounting firms;
4. conduct investigations and disciplinary proceedings, and impose appropriate sanctions;
5. enforce compliance with the Act, the rules of the Board, professional standards, and the securities laws relating to the preparation and issuance of audit reports and the obligations and liabilities of accountants with respect thereto;
6. set the budget and manage the operations of the Board and the staff of the Board;
7. perform such other duties or functions as necessary or appropriate.

PCAOB is required to "cooperate on an on-going basis" with designated professional groups of accountants and any advisory groups convened in connection with standard-setting. The Board must adopt an audit standard to implement the internal control review required by Subsection 404(b) of SOX. Thus, PCAOB acts in a similar role as the Registrar Accreditation Board (RAB) and the other members of the International Accreditation Forum (IAF) do with QMS and EMS registrars.

An example of a professional group with which PCAOB must cooperate is the Committee of Sponsoring Organizations (COSO) of the National Commission on Fraudulent Financial Reporting, popularly known as the Treadway Commission. The five major US financial professional associations—American Accounting Association (AAA), AICPA, Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA)—are members of COSO.

By early 2004, the PCAOB must provide a guidance document on implementing Section 404, which appears on page 16 and is discussed below. Using COSO guidance as a starting point, PriceWaterhouseCoopers developed a draft "Enterprise Risk Management Framework" for internal controls on behalf of COSO, which completed a 90-day period of public review on October 14, 2003.

The new framework builds on COSO's previously issued framework, "Internal Control—Integrated Framework" and identifies the interrelationships between enterprise risk management, internal control and entity management. This document continues to reinforce the notion that financial, quality and environmental auditors need to understand risk management, implement it in their audit plans and communicate "enterprise risks" to the highest company levels. To obtain information about COSO and its work, visit its web site (www.coso.org).

Section 103 relates to the Board, the certified public accountants (CPAs) and the reports these CPAs will issue to public companies, but it is important to understand what Section 103 specifies and how it will impact on financial audits of your company and what your

(page 17, SARBANES-OXLEY)

SELECTED DEFINITIONS AND SECTION 103

Section 2. Definitions.

(2) Audit.—The term "audit" means an examination of the financial statements of any issuer by an independent public accounting firm in accordance with the rules of the Board or the Commission (or, for the period preceding the adoption of applicable rules of the Board under section 103, in accordance with then-applicable generally accepted auditing and related standards for such purposes), for the purpose of expressing an opinion on such statements.

(3) Audit committee.—The term "audit committee" means—

(A) a committee (or equivalent body) established by and amongst the board of directors of an issuer for the purpose of overseeing the accounting and financial reporting processes of the issuer and audits of the financial statements of the issuer; and

(B) if no such committee exists with respect to an issuer, the entire board of directors of the issuer.

(4) Audit report.—The term "audit report" means a document or other record—

(A) prepared following an audit performed for purposes of compliance by an issuer with the requirements of the securities laws; and

(B) in which a public accounting firm either—

(i) sets forth the opinion of that firm regarding a financial statement, report, or other document; or

(ii) asserts that no such opinion can be expressed.

(10) Professional standards.—The term "professional standards" means—

(A) accounting principles that are—

(i) established by the standard setting body described in section 19(b) of the Securities Act of 1933, as amended by this Act, or prescribed by the Commission under section 19(a) of that Act (15 U.S.C. 17a(s)) or section 13(b) of the Securities Exchange Act of 1934 (15 U.S.C. 78a(m)); and

(ii) relevant to audit reports for particular issuers, or dealt with in the quality control system of a particular registered public accounting firm; and

(B) auditing standards, standards for attestation engagements, quality control policies and procedures, ethical and competency standards, and independence standards (including rules implementing title II) that the Board or the Commission determines—

(i) relate to the preparation or issuance of audit reports for issuers; and

(ii) are established or adopted by the Board under section 103(a), or are promulgated as rules of the Commission.

Section 103. Auditing, Quality Control, and Independence Standards and Rules.

(a) Auditing, Quality Control, and Ethics Standards.—

(1) In general.—The Board shall, by rule, establish, including, to the extent it determines appropriate, through adoption of standards proposed by 1 or more professional groups of accountants designated pursuant to paragraph (3)(A) or advisory groups convened pursuant to paragraph (4), and amend or otherwise modify or alter, such auditing and related attestation standards, such quality control standards, and such ethics standards to be used by registered public accounting firms in the preparation and issuance of audit reports, as required by this Act or the rules of the Commission, or as may be necessary or appropriate in the public interest or for the protection of investors.

(2) Rule requirements.—In carrying out paragraph (1), the Board—

(A) shall include in the auditing standards that it adopts, requirements that each registered public accounting firm shall—

(i) prepare, and maintain for a period of not less than 7 years, audit work papers, and other information related to any audit report, in sufficient detail to support the conclusions reached in such report;

(ii) provide a concurring or second partner review and approval of such audit report (and other related information), and concurring approval in its issuance, by a qualified person (as prescribed by the Board) associated with the public accounting firm, other than the person in charge of the audit, or by an independent reviewer (as prescribed by the Board); and

(iii) describe in each audit report the scope of the auditor's testing of the internal control structure and procedures of the issuer, required by section 404(b), and present (in such report or in a separate report)—

(I) the findings of the auditor from such testing;

(II) an evaluation of whether such internal control structure and procedures—

(aa) include maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;

(bb) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and

(III) a description, at a minimum, of material weaknesses in such internal controls, and of any material noncompliance found on the basis of such testing.

(next page, SECTION 103)

SECTION 103 (CONT.)

(B) shall include, in the quality control standards that it adopts with respect to the issuance of audit reports, requirements for every registered public accounting firm relating to—
  (i) monitoring of professional ethics and independence from issuers on behalf of which the firm issues audit reports;
  (ii) consultation within such firm on accounting and auditing questions;
  (iii) supervision of audit work;
  (iv) hiring, professional development, and advancement of personnel;
  (v) the acceptance and continuation of engagements;
  (vi) internal inspection; and
  (vii) such other requirements as the Board may prescribe, subject to subsection (a)(1).

(3) Authority to adopt other standards.—
  (A) In general.—In carrying out this subsection, the Board—
    (i) may adopt as its rules, subject to the terms of section 107, any portion of any statement of auditing standards or other professional standards that the Board determines satisfy the requirements of paragraph (1), and that were proposed by 1 or more professional groups of accountants that shall be designated or recognized by the Board, by rule, for such purpose, pursuant to this paragraph or 1 or more advisory groups convened pursuant to paragraph (4); and
    (ii) notwithstanding clause (i), shall retain full authority to modify, supplement, revise, or subsequently amend, modify, or repeal, in whole or in part, any portion of any statement described in clause (i).
  (B) Initial and transitional standards.—The Board shall adopt standards described in subparagraph (A)(i) as initial or transitional standards, to the extent the Board determines necessary, prior to a determination of the Commission under section 101(d), and such standards shall be separately approved by the Commission at the time of that determination, without regard to the procedures required by section 107 that otherwise would apply to the approval of rules of the Board.
  (4) Advisory groups.—The Board shall convene, or authorize its staff to convene, such expert advisory groups as may be appropriate, which may include practicing accountants and other experts, as well as representatives of other interested groups, subject to such rules as the Board may prescribe to prevent conflicts of interest, to make recommendations concerning the content (including proposed drafts) of auditing, quality control, ethics, independence, or other standards required to be established under this section.

(b) Independence Standards and Rules.—The Board shall establish such rules as may be necessary or appropriate in the public interest or for the protection of investors, to implement, or as authorized under, title II of this Act.

(c) Cooperation With Designated Professional Groups of Accountants and Advisory Groups.—
  (1) In general.—The Board shall cooperate on an ongoing basis with professional groups of accountants designated under subsection (a)(3)(A) and advisory groups convened under subsection (a)(4) in the examination of the need for changes in any standards subject to its authority under subsection (a), recommend issues for inclusion on the agendas of such designated professional groups of accountants or advisory groups, and take such other steps as it deems appropriate to increase the effectiveness of the standard setting process.
  (2) Board responses.—The Board shall respond in a timely fashion to requests from designated professional groups of accountants and advisory groups referred to in paragraph (1) for any changes in standards over which the Board has authority.

(d) Evaluation of Standard Setting Process.—The Board shall include in the annual report required by section 101(h) the results of its standard setting responsibilities during the period to which the report relates, including a discussion of the work of the Board with any designated professional groups of accountants and advisory groups described in paragraphs (3)(A) and (4) of subsection (a), and its pending issues agenda for future standard setting projects.

Section 404. Management Assessment of Internal Controls.

(a) Rules Required.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—
  (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
  (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) Internal Control Evaluation and Reporting.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

SARBANES-OXLEY

(from page 14)

QMS and/or EMS can do to ensure the audits and the reports relate to accurate data.

Section 404: Management Assessment of Internal Controls

This section (reprinted on previous page) requires each annual report to contain an "internal control report", the requirements of which are spelled out in (1) and (2) of Subsection 404(a). In addition, the registered public accounting firm that audits a company and will prepare or issue the financial report signed by the company's CEO and CFO must attest to, and report on, the assessment made by the management of the company.

In effect, what Section 404 really requires is effective management of the company's financial information by its Top Management—or by the financial personnel under the direction and oversight of Top Management—so that the financial statements that result from the auditing of the financial information are credible. From a QMS and/or EMS viewpoint, this section of SOX requires the accounting firm to act as third-party auditors of the procedures and controls the company has in place to ensure that the financial operations output metrics are correct and effective in conveying the financial health of the company.

Section 302: Corporate Responsibility for Financial Reports

Quality—and perhaps environmental—professionals have often felt that Top Management, particularly the CEOs and CFOs, does not frequently understand and pay much attention to the QMSs and EMSs in many organizations because the members of Top Management are primarily focused on the financial aspects of the organization. However, Section 302 (reprinted below) puts the responsibility for the reports on the financial aspects of the organization in public companies squarely in the hands of the CEO and CFO. They have to prepare a statement to accompany each periodic financial report certifying the appropriateness of the financial statements and disclosures that are contained in the report.

And subsection (a)(3) requires those financial statements to "fairly present in all material respects the financial condition and results of the issuer as of, and for, the periods presented in the report;...." The obvious intent of SOX rests in Section 302, which puts Top Management at risk of criminal penalties (e.g., federal prosecution for violating SOX) and civil penalties (e.g., liability lawsuits from investors) if the "signing officers" knowingly and/or

(next page, SARBANES-OXLEY)

Section 302. Corporate Responsibility for Financial Reports.

(a) Regulations Required.—The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m, 78o(d)), that the principal executive officer or officers and the principal financial officer or officers, or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—

(1) the signing officer has reviewed the report;

(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;

(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;

(4) the signing officers—

(A) are responsible for establishing and maintaining internal controls;

(B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

(C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and

(D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—

(A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls; and

(B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

(b) Foreign Reincorporations Have No Effect.—Nothing in this section 302 shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302, by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.

(c) Deadline.—The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act.

SARBANES-OXLEY

(from previous page)

intentionally allowed an untrue statement to appear in the financial reports or allowed relevant information to be omitted. Further, subsection (4) reinforces the CEO and CFO responsibilities for the procedures within the company that are to ensure accurate financial statements are generated. Thus, the financial auditors are enabled to provide accurate audit reports, but primary responsibility for any failure to comply with SOX is in Top Management's hands.

Since August 2002, when the CEOs and CFOs of public companies in the United States—and of those firms reincorporated to a location outside the United States—became obligated to review and sign off on quarterly and annual financial reports to comply with SOX, there have been a number of "restatements" of financial information for companies covering reports in the past few years. In fact, an article by Carrie Johnson in *The Washington Post* ("Fewer Firms Restated Financial Results in 2003", January 13, 2004) reported that the Huron Consulting Group LLC, a Chicago-based forensic accounting and turnaround firm, reported on January 12 that "323 public companies changed their previously released financial reports because of accounting errors and irregularities last year, down from 330 in 2002."

In the article, Johnson wrote that "Huron said the 'leading cause' for financial restatement last year was mistakes and improprieties in how companies booked reserve and contingency accounts." Of the restatements in 2003, 63% involved changes to annual financial reports filed with the SEC. While not all these restatements are a result of SOX, some may very well be. And although there has not yet been a report of a noncompliance that resulted in the bringing of charges against the signing officers of a company that submitted its financial reports—restatements could be a response in line with the requirements of Section 409 discussed below—the risk remains that such prosecutions will eventually occur.

Section 409: Real Time Issuer Disclosures

Section 409 (reprinted below) makes clear that the CEO and CFO do not have until the next regularly scheduled financial report to disclose to the public significant changes in the financial condition of the company, including its operations. This may be a reaction to the delay in reporting by Enron's executives of financial difficul-

(next page, SARBANES-OXLEY)

Section 409. Real Time Issuer Disclosures.

Section 13 of the Securities Exchange Act of 1934 (15 U.S.C. 78m), as amended by this Act, is amended by adding at the end the following:

"(l) Real Time Issuer Disclosures.—Each issuer reporting under section 13(a) or 15(d) shall disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the issuer, in plain English, which may include trend and qualitative information and graphic presentations, as the Commission determines, by rule, is necessary or useful for the protection of investors and in the public interest."

Sec. 906. Corporate Responsibility for Financial Reports.

(a) In General.—Chapter 63 of title 18, United States Code, is amended by inserting after section 1349, as created by this Act, the following:

"**§ 1350. Failure of corporate officers to certify financial reports**

"(a) Certification of Periodic Financial Reports.—Each periodic report containing financial statements filed by an issuer with the Securities Exchange Commission pursuant to section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a) or 78o(d)) shall be accompanied by a written statement by the chief executive officer and chief financial officer (or equivalent thereof) of the issuer.

"(b) Content.—The statement required under subsection (a) shall certify that the periodic report containing the financial statements fully complies with the requirements of section 13(a) or 15(d) of the Securities Exchange Act pf 1934 (15 U.S.C. 78m or 78*o*(d)) and that information contained in the periodic report fairly presents, in all material respects, the financial condition and results of operations of the issuer.

"(c) Criminal Penalties.—Whoever—

"(1) certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than $1,000,000 or imprisoned not more than 10 years, or both; or

"(2) willfully certifies any statement as set forth in subsections (a) and (b) of this section knowing that the periodic report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than $5,000,000, or imprisoned not more than 20 years, or both."

(b) Clerical Amendment.—The table of sections at the beginning of chapter 63 of title 18, United States Code, is amended by adding at the end the following: "1350. Failure of corporate officers to certify financial reports."

SARBANES-OXLEY

(from previous page)

ties, but Section 409 places the imperative on every public company to have procedures in place to immediately communicate to the public about changes that could impact on investment and purchasing decisions. The fact is that few such companies would not benefit from careful monitoring of their financial condition and operations, which would identify situations where corrective action is needed and where some restatements could be avoided.

It is clear that the requirements of SOX will have a major effect on the management of companies and that their QMSs and EMSs will have a major role to play. As noted above, the reason for this major role is that these systems are already present in many companies and either already are or could easily be equipped to ensure financial statements are accurate and can quickly be updated to address operational conditions and help satisfy Section 409.

Section 906: Responsibility for Financial Reports

Finally, Section 906 (reprinted on previous page) amends Chapter 63 of Title 18 of the United States Code to specify penalties to be faced by CEOs and CFOs should a certified period report contain any statement that does not accurately represent the financial condition and results of operations of the organization. Top Management will pay a great deal of attention to this section because it lays out criminal penalties for (a) criminal negligence and (b) intent to deceive. For "criminal negligence", the perpetrator can receive a fine of up to $1 million and a jail sentence of up to 10 years. For "intent to deceive", the penalties increase to up to $5 million and 20 years. Perhaps these penalties could have prevented the Enron and WorldCom scandals.

The Effect of SOX on the Management of US Organizations

There has been a shift in what has served as the primary filter through which Top Management in US corporations reached decisions. In the past, it was cost, quality and customer satisfaction that served as the filter. Then, quality and customer satisfaction lost their top roles and costs and schedules became the primary management decision filter. This was brought on by the pressures of increasing competition and first-to-market demands. Evidently, the filter has changed once again.

"Since 9/11, risk and its management is now the primary filter by which top management makes decisions," wrote Greg Hutchins in his October 2002 *Quality Digest* article. The risks to Top Management, as defined by SOX, from making false financial statements—either knowingly or unknowingly, since the signing officers are responsible for both reviewing the statements for accuracy and ensuring that the internal controls exist and are used to ensure accuracy—simply add to the risk Hutchins referred to.

I have identified four key aspects that are mandated by SOX for a public company that strongly affect the management of all organizations. That is because they are important to the effective management of any organization, whether or not SOX applies. The four are:

1. Internal Controls—SOX requires a system of internal controls that may be satisfied by the integrated framework defined by COSO, which is reprinted in

(next page, SARBANES-OXLEY)

The COSO Definition of Internal Control (Excerpts)

Internal control is broadly defined as a process, effected 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:

1. Effectiveness and efficiency of operations.
2. Reliability of financial reporting.
3. Compliance with applicable laws and regulations.

Internal control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. Although the components apply to all entities, small and mid-size companies may implement them differently than large ones. Its controls may be less formal and less structured, yet a small company can still have an effective internal control process. The components are:

- **The Control Environment**...is the foundation for all other components of internal control, providing discipline and structure.
- A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. **Risk Assessment** is the identification and analysis of relevant risks to the achievement of objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will change, mechanisms are needed to deal with the special risks associated change.
- **Control Activities** are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to the achievement of the entity's objectives.
- **Information and Communication**—Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting.
- Internal control systems need to be **monitored**—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties.

SARBANES-OXLEY

(from previous page)

the sidebar below. As discussed above, COSO is in the process of updating this to an "Enterprise Risk Management Framework" that goes beyond mere compliance and focuses on risk management. Note that the COSO definition of internal control can be structured as a PDCA improvement process: Plan—control environment; Do—information and communication; Check—risk assessment and monitoring; and Act—control activities.

2. Corporate Records—Current legal requirements related to SOX include those on maintaining corporate books and records and internal auditing processes. In 1977, the Foreign Corrupt Practices Act (FCPA) imposed direct regulation designed to ensure that public companies can meet their financial disclosure obligations. According to Chapter 2, Recommendations for Public Companies, of the 1977 "Report of the National Commission on Fraudulent Financial Reporting", which is available on COSO's web site, public companies are required to keep books and records that reflect their transactions and assets accurately and fairly and to maintain a system of internal accounting control that enables them to prepare financial statements in conformity with Generally Accepted Accounting Principles (GAAP). GAAP is the set of accounting principles used by all US public companies and many companies worldwide. Unfortunately, GAAP is not comprehensive, especially in matters that QMSs and EMSs may deal with. In "Inside Track with Broc: Greg Rogers on Environmental Liabilities Risks and Disclosure" that was posted October 20, 2003, on a legal web site (www.thecorporatecounsel.net), Rogers wrote that "there are several gaps in GAAP with regard to environmental [and quality] matters, and many companies have adopted financial reporting policies and procedures that tend to understate these liabilities."

3. Internal Financial Audit Function—All public companies must have an effective and objective internal financial audit function. Internal financial auditor qualifications, the auditing staff and their status within the company, the reporting lines for the results of internal financial audits and the relationship of the auditing staff with the audit committee of the board of directors must be adequately defined and sufficiently robust to ensure the effectiveness and objectivity of the internal audit function. In its Summary of Recommendations, the "Treadway Report" noted that the internal auditor should consider his/her audit findings in the context of the company's financial statements and should, to the extent appropriate, coordinate his/her activities with the activities of the independent public accountant. This is a practical approach, since this function is the ultimate internal control on which the CEO and CFO are relying for compliance with SOX and for assurance when signing off on financial statements.

4. The Audit Committee—Historically, the audit committee of a public company's board of directors has provided the oversight and monitored the management of the financial audit function and of the outside auditor. SOX requires internal controls that in effect require all public companies to strengthen that historical role. After all, the audit committee plays a role critical to the integrity of a company's financial reporting. The Treadway Commission also recommended in the Report that all public companies be required to have audit committees composed entirely of independent directors. To be effective, audit committees should exercise vigilant and informed oversight of the financial reporting process, including the company's internal controls. The board of directors should set forth the committee's duties and responsibilities in a written charter. Among other things, the audit committee should review management's evaluation of the independence of the public accountant and management's plans for engaging the company's independent public accountant to perform management advisory services (not to be confused with financial consulting services). The Treadway Report highlighted additional important audit committee duties and responsibilities in the course of discussing other recommendations affecting public companies.

Logical SOX Conclusion: Use Your Management Systems

To recap, the financial management and reporting problems at Enron, WorldCom and other organizations have led to the passage of the Sarbanes-Oxley Act of 2002. SOX requires specific governance procedures for public companies, including the attestation (affirmation) by the CEO and CFO of the financial statements of those companies.

The primary filter and concern for Top Management is now risk. The risks include not being able to meet requirements, undesirable events and their consequences, the effects of operational variation from specifications or customer requirements and failure to provide accurate information about the company in financial statements to the SEC. I have reviewed five sections of SOX and the implications of their requirements for the financial operations and reporting of a public company. As noted above, valuable tools already exist in many companies that must comply with SOX and these tools—such as ISO 9001-conforming QMSs and ISO 14001-conforming EMSs—could be effectively used in most instances without a significant change to the organization. But knowing how to harness these tools in a cost-effective way is important.

This is the first of three articles discussing how QMSs and EMSs can support internal financial auditing in response to the requirements of SOX. The second article will examine how a company can combine its QMS and EMS "tools" with its financial auditing function and its procedures to provide Top Management and the board of

(next page, SARBANES-OXLEY)

SARBANES-OXLEY

(from previous page)

directors with an accurate understanding of the organization's status. Both ISO 9001 and ISO 14001 require organizations to continually improve their systems, and the goal of combining the management systems with the auditing function is to use the system's continual improvement processes to create a more effective organization.

Enabling the CEO and CFO to sign off on the financial statements with a good understanding of their accuracy is part of that goal. A by-product will be the ability of Top Management to identify business risks, control them and prevent major surprises. Indeed, the end result will be the creation of a combined financial, quality and environmental auditing process that establishes a framework for overall improvement and will result in better results for all stakeholders. ###

[Editor's Note: A team was recently formed to develop an understanding of the relationship between financial and quality/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 (e-mail: sandfordl@msn.com).*

***Lawrence Liebesman**, Partner, Environmental Practice, Holland & Knight LLP (e-mail: lliebesman@hklaw.com).*

***Paul Palmes**, Quality Assurance Director, Northern Pipe Products Inc. (e-mail: paulp@northernpipe.com).*

***John Walz**, Quality Management System Consultant (e-mail: johnwalz@ameritech.net).*

QuEST FORUM

(from page 10)

Best Practices Conference will be held September 21-22, 2004, in Richardson, TX. For more information on the QuEST Forum, visit its web site (www.questforum.org) or contact the QuEST Forum administrator (questforum@asq.org). *THE OUTLOOK* will provide coverage of developments involving use of TL 9000 and the TL 9000 indices and of the next release of the QMS Requirements and Measurements Handbooks in upcoming issues. ###

OTHER NEWS ITEM OF INTEREST

2nd Edition of IWA-1 Due in 2004, No Changes to Main Text Likely

Hospitals and other health services providers that have held off implementing an ISO 9001:2000-conforming QMS pending changes in the second edition of *International Workshop Agreement (IWA) 1, Quality management systems—Guidelines for process improvements in health service organizations*, are advised to use the first edition since the second edition is unlikely to have significant changes.

The US Experts responsible for the initial documents that led to the development of IWA-1 report that the first edition of IWA-1 was reviewed by a panel of mostly doctors (MDs) and registered nurses and that the comments from this review panel were collected and put into a draft template for the Executive Team to review and make comments.

The Executive Team consists mainly of members from the executive team that organized the January 2001 workshop in Detroit that produced IWA-1. "We compiled the comments on IWA-1:2001 and the main change that may come out of this is a slight change to the format, with some additional notes on 'What to Look For' and 'Guidance'," explained Mickey Christensen, who was a member of the original Executive Team for the workshop that produced IWA-1 and is a leading figure on the new Team. "These two paragraph headings are disbursed throughout the document as needed."

Following a January 2004 meeting of the Executive Team, Christensen told *THE OUTLOOK* that "the main wording of the document basically has not changed, since we asked that the original intent and content not be changed significantly from what the 2001 workshop attendees approved by an 89% favorable vote. The executive team will consider the draft and then, in a reasonably short period of time, a decision will be made as to whether this draft should progress in the process or to just confirm to ISO that the document should stand as originally published for another three years.

"Our goal is to have the draft approved and published by September 2004 or to have the current IWA-1 continued as-is," said Christensen. *THE OUTLOOK* will provide another update once the Executive Team has made a decision. ###