



## STANDARDS

# Sarbanes-Oxley And ISO 9000

by **William A. Stimson**

**A**lmost from its inception, critics have denounced ISO 9000 as being strong on form and short on substance. In many comparisons, the international standard trails far behind such robust quality programs as Malcolm Baldrige National Quality Award criteria, lean and Six Sigma. Typically, the criticism is aimed at what seems to be ISO 9001's plethora of documentation requirements.

From the legal point of view, however, documentation is a major asset of ISO 9001, providing records and internal controls. For example, a test result is a record. A signature is a control. Quality records define a trail from customer expectations to delivery and all steps in between.

This trail assumes massive importance when customer disappointment goes to court. Indeed, fol-

lowing the collapse of customer confidence in the aftermath of major corporate scandals, the U.S. government has gotten very interested in paper trails and controls. In law, they are not form but substance, and you can go to jail if the trail is not clear. In the past, a company might have to pay a fine for wrongdoing, but under the Sarbanes-Oxley Act of 2002 (SOX),<sup>1</sup> the CEO can go to prison as well.

### **Sarbanes-Oxley**

SOX is the U.S. government's response to the financial scandals at Enron, WorldCom, Tyco and other large companies under the purview of the Securities and Exchange Commission (SEC). Composed of 11 titles, as shown in Table 1, the act mandates strict requirements for financial accounting of public companies and transforms the public accounting industry.

In reforming disclosure procedures and corporate governance, the various titles and sections of SOX define management responsibilities in annual and quarterly reports, the control environment, risk management, and monitoring and measuring control activities.

SOX is a law, not a standard. It tells you what to do but provides no guidelines on how to do it. Hence, many companies are adopting the risk management framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO)<sup>2</sup> as a standard of compliance to SOX.

COSO was formed in 1985 to support the National

### **In 50 Words Or Less**

- **Critics say ISO 9000 doesn't compare favorably to quality programs such as the Baldrige criteria, lean and Six Sigma.**
- **But ISO 9001's emphasis on documentation is a major asset from a legal perspective.**
- **Quality professionals can help companies comply with Sarbanes-Oxley while enhancing their organizational status.**

**TABLE 1** The 11 Titles of Sarbanes-Oxley

Table of contents	Subject title
Title I	Public Company Accounting Oversight Board
Title II	Auditor independence
Title III	Corporate responsibility
Title IV	Enhanced financial disclosures
Title V	Analyst conflicts of interest
Title VI	Commission resources and authority
Title VII	Studies and reports
Title VIII	Corporate and criminal fraud accountability
Title IX	White-collar crime penalty enhancements
Title X	Corporate tax returns
Title XI	Corporate fraud and accountability

Commission on Fraudulent Financial Reporting, an independent private sector initiative. The sponsors are major professional financial associations in the United States, and the commission has representatives from industry, public accounting, investment firms and the New York Stock Exchange.

### SOX and ISO 9001

Many observers have noticed the similarity between ISO 9001 and the SOX requirements of internal control and believe companies that are ISO 9001 certified/registered have a framework in place that can be emulated to meet these requirements.

For example, ISO 9001 offers a single and complete set of managed and applied procedures. The procedures are distributed where needed, regularly updated and audited. SOX requires similar characteristics.

It would be relatively simple to piggyback accounting procedures and audits on the already existing ISO 9001 framework. Jim Mroz, former editor of *The Informed Outlook*, endorsed this idea, pointing out that SOX presents an opportunity to merge the procedures and internal audits of financial processes with those of quality systems.<sup>3</sup> By emulating ISO 9001 in their financial and information activities, companies can gain compliance with SOX and achieve a seamless and effective integration of all critical corporate activity.

The relationship between SOX and ISO 9001 is two way. SOX can benefit by emulating ISO 9001, but ISO 9001 can also benefit by emulating SOX. Indeed, careful reading of the Sarbanes-Oxley Act

suggests SOX criteria may be applied to ISO 9000 in the not too distant future. The driving force connecting SOX to quality is the cost of quality factor.

### Cost of Quality

Joseph Juran recognized the technical language of production, such as defect rates, out of specs and failure modes, would probably not attract the attention of executive management. He advocated a cost of quality accounting system<sup>4</sup> that expressed quality in terms of money, and he classified the types of costs as failure, appraisal and prevention, sometimes referred to by the acronym FAP.

This perspective is exact but does not go far enough. For example, an appraisal cost might be an assessment of material condition. A failure cost might be defects discovered before shipment. Unfortunately, the analysis of FAP takes us back to technical language, although in terms of costs.

Costs of quality are sometimes translated into financial measures of quality, a term that reveals its association to SOX. This perspective allows quality professionals to express the costs of quality in terms related to the company's strategic objectives. For example:

1. Net income includes net sales less operating expenses.
2. Operating expenses include cost of quality factors.
3. Total assets include accounts receivable plus all inventory, including in-process inventory.
4. Return on total assets is the ratio of net income to total assets.
5. Net income affects the company's market value.

Objective four is a measure of profitability and relates directly to the company's strategic goals. However, objective five is the factor that will most quickly catch the attention of auditors subject to the SOX law. A misstatement here can mean jail time for CEOs. Quality falls under the purview of SOX when the costs of quality—operating costs and inventory—are expressed in terms of profitability and market value.

Working with production and financial accounting, the quality manager can help keep the organization in conformance to SOX and at the same time gain for quality a preeminence in the organization that has been missing for a very long time.

### SOX Applied to the Cost of Quality

Top management should anticipate the areas of direct application of SOX to the cost of quality: governance, operations and IT. Let's look at the wording.

**Governance.** There is no universal agreement on

what “corporate governance” means, but a definition used by the Organization for Economic Cooperation and Development (OECD) is becoming internationally accepted:

A system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of responsibilities and rights among different participants in the corporation, such as the board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs. By doing this, it also provides the structure through which the company objectives are set, and the means of attaining those objectives and monitoring performance.<sup>5</sup>

SOX does not use the word “governance” per se, but the management responsibilities listed in Titles III, IV, V, VIII, IX and XI exactly fit the OECD definition of governance. They apply to all public companies. Narrowly interpreted, SOX refers only to financial processes, but this perspective will broaden to operations because of the cost of quality.

Cost of quality refers to quality processes, but such processes have a new meaning with the advent of ISO 9000: 2000. “Quality processes” does not apply to quality assurance. It applies to all the value adding processes of production and service of an organization and can be construed to apply to its support services as well.

Thus, the cost of quality permeates an organization and has a direct influence on its bottom line, which under Section 302 of SOX must be honestly reported on pain of criminal penalty. At some level of aggregation, the various activities of an organization add up to unity, and that level is corporate governance.

**Operations.** Title I of SOX refers frequently to quality control, policies and procedures. You might assume this refers to the quality of financial processes, but Titles III and IV broaden the scope.

In Section 302, the CEO and CFO of a public company are charged with certifying their financial condition in quarterly and annual reports. Section 404 requires the CEO to accept responsibility for the effectiveness of internal financial controls. If a control affects the cost of quality, then it follows CEO verification of all operational controls cannot be long in coming. Top management may be legally responsible for effective and efficient quality control.

**IT Systems.** Financial data and procedures are

usually embedded in a company’s IT system. Rules for IT management that ensure SOX compliance are described in the IT Control Objectives for Sarbanes-Oxley,<sup>6</sup> a product of the IT Governance Institute. Therefore, the IT department also must comply with SOX.

It is expensive and inefficient to maintain two IT systems, one for finance and another for production and service, particularly when all the activities are interrelated. A single, comprehensive and certifiable IT system is the solution.

Unintentionally or not, many companies have maintained mirror systems: one for production and one for ISO 9001; one for IT and one for quality; one for engineering and one for quality assurance, with marginal interface among them. This inefficiency has contributed to waste and cost. Under SOX, it may lead to prison.

So, the SOX criteria may be applied to ISO 9001 on the grounds that a quality audit can be as critical to company investors as a financial audit, if the cost of quality is a material factor in company earnings or if ISO 9001 compliance and conformance is a material factor in contract award and performance.

### SOX Applied to ISO 9000

Each title of the Sarbanes-Oxley Act contains several sections, which are numbered to correspond to their titles. For example, Section 302 is located under Title III; Section 805 is located under Title VIII. Not all the sections are applicable to ISO 9001, although most of the titles can apply in some sense.

The 11 titles and their relationship to ISO 9001 are shown in Table 2. ISO 9001 is already in or near compliance to five of the titles because it uses an equivalent function. In the remaining titles, there is a direct application in meaning or the spirit of the law. For example, SOX establishes a board for oversight of public accountability. ISO 9001 has an equivalent board in place—the ANSI-ASQ National Accreditation Board (ANAB). (Note: Until its recent restructuring, ANAB was generally known as the Registrar Accreditation Board.) **Title I—Public Company Accounting Oversight Board (PCAOB).** This title establishes a board and provides the authority to administer the financial audit of public companies. An equivalent board under ISO 9000 would be empowered to administer the quality audit of public companies. Since such a board—ANAB—already exists, ISO 9000 is already in compliance with Title I.



**Title II—auditor independence.** Section 201 prohibits an audit firm from performing a contemporaneously nonaudit service to a client company. The client company can waive this restriction only if such waiver is announced to investors and if the value of the nonaudit service is less than 5% of the audit service.

Section 203 rotates the lead auditor every five years. Section 204 requires the audit team to report its rules and procedures to the client company's audit committee. Section 206 deals with conflict of interest by prohibiting any recent former employees of the audit firm from serving in a top management role for the client company. Section 207 rotates the audit firms certifying a client company. (This section is still under review.) And Section 209 empowers state regulators to determine whether PCAOB's requirements are applicable to companies of all sizes.

The sections of Title II are shown here in considerable detail so readers can see how pertinent SOX requirements are to the quality world. ISO 9001 is almost in compliance to Title II because ANAB is empowered to define audit rules. Yet, there is an important caveat: Under SOX, ANAB could not permit its registrars to offer consulting services to companies it audits. So ISO 9000 is near, but not in, compliance to Title II.

**Title III—corporate responsibility.** Section 301 requires a company to establish an independent, top management audit committee. Section 302 requires certification of the audit report as true by top management. Section 303 prohibits executive management from improper influence of an auditor in a financial audit report.

**TABLE 2** Comparison of Sarbanes-Oxley and ISO 9000

Title	ISO 9001 equivalent	ISO 9001 application	Duties
I. Public Company Accounting Oversight Board	Registrar Accreditation Board (RAB)	In compliance	Administer accreditation program
II. Auditor independence	RAB	Near compliance	Define audit rules
III. Corporate responsibility	Management review (clause 5.6.2)	Company executive audit committee	1. Certify audit report as true. 2. Respect auditor independence. 3. Certify compliance (clause 4.2.2).
IV. Enhanced financial disclosures	None	Management responsibility: quality management system conformance	1. Certify internal controls (clause 4.1), effectively certify conformance. 2. Adhere to code of ethics. 3. Be open to customers (clauses 4.1 and 7.1).
V. Analyst conflicts of interest	Customer focus (clause 5.2)	In compliance	Put customer interests first (clauses 5.2 and 7.2).
VI. Commission resources and authority	RAB	In compliance	Set professional standards.
VII. Studies and reports	RAB	In compliance	Consolidate registrars and standards.
VIII. Corporate and criminal fraud accountability	None	Management responsibility: records/documents	Retain honest records (clauses 4.2 and; 8.0). Protect employees.
IX. White-collar crime penalty enhancements	None	Management responsibility: reports/documents	Retain honest reports (clauses 4.2 and 8.0).
X. Corporate tax returns	None	None	None
XI. Corporate fraud accountability	None	Management responsibility: records/documents	Retain honest reports (clauses 4.2 and 8.0). Criminal penalties for false reports needed in legal proceedings.

Applied to ISO 9001, clause 5.1, Title III would create a top management audit committee with responsibility for the outcome of an ISO 9001 audit. This function already exists in ISO 9001 under the internal audit requirements of clause 8.2.2 and the management review of clause 5.1. Title II requires respect for auditor independence, which would apply to third-party auditors. An organization might challenge the audit—this happens quite often—but it could not improperly influence the auditors' findings.

How about certifying a financial report? Is there an ISO 9000 equivalent? The closest thing quality

has to a financial report is its quality manual, which is not much of a stretch when you think about it.

The financial report attests to the health of the company finances and compliance to SOX. The quality manual is effectively a report of the company quality management system (QMS). It attests to the health of the company quality system and compliance to ISO 9001.

It has monetary value, too, because it can be the basis for winning a bid. If you win a bid because you're ISO 9001 certified/registered and your quality manual is not in compliance, that's possible fraud. A SOX based ISO 9001 system would require the CEO to certify compliance of the company quality manual to ISO 9001.

## An existing ISO 9000 structure lends itself to integration with a company's financial system.

One could argue ISO 9001 compliance is already certified by a registrar. Under SOX, an organization could not use this argument as a defense for non-compliance any more than it can now use the certification of a public accounting firm. Based on clause 5.6.1 of ISO 9001, Title III of SOX would require executive certification of the QMS as in compliance.

### **Title IV—enhanced financial disclosures.**

Section 404 requires top management to assess whether an internal control is working properly. Quality systems also have controls, although calling them that has dropped out of favor. For example, a measurement is a control. It tells you whether an attribute or value is acceptable.

Sometimes a signature is a control. In ISO 9001, clause 4.1.c, this section would assign responsibility of process controls to top management. What exactly does this mean? Is it an outrageous demand on management? Well, Japanese managers do it all the time. Masaaki Imai exhorts all managers, "Go to *gemba!* Go to the workplace and see what's going on!" SOX tells top management, "You are responsible for how well your processes work."

Section 406 requires a code of ethics for finan-

cial officers. The nearest ISO 9000 gets to this is ISO 9004, clause 5.1.1, which is not contractual. It could be argued, however, that a code of ethics is an intrinsic part of professionalism, and that the requirement for a code of ethics for management is within the purview of ISO 9001, clause 5.0.

Section 409 requires real-time disclosure of pertinent financial *or operational* changes. Obviously, this report might influence the market price of corporate stock. Material operational changes may also affect contract performance and so should be disclosed to the customer in real time. Applied to ISO 9001, clauses 4.1.f or 7.1.f, this section would provide visibility to customers and shareholders.

**Title V—analyst conflicts of interest.** Section 501 requires rules to prevent analysts from making recommendations in their own interests and not in that of the investor. Applied to ISO 9001, clause 7.2, this would put customer interests first, which is already required in ISO 9001 under customer focus. So ISO 9001 is already in compliance to Title V.

**Title VI—commission resources and authority.** This title refers to the SEC. In ISO 9000, it would apply to ANAB. Because this organization is already funded for its roles and has the authority to set professional standards, ISO 9001 is already in compliance to Title VI.

**Title VII—studies and reports.** This title refers to the consolidation of public accounting firms. In ISO 9000, this title would apply to ANAB, which has the authority to consolidate registrars and standards. So ISO 9000 is already in compliance to Title VII.

**Title VIII—corporate and criminal fraud accountability.** Title VIII differs from the others in that it applies to both public and private companies.<sup>8</sup> It refers to the destruction of valid records and the creation of fraudulent ones, retention of records, whistleblowing protection, prohibition of threats and harassment against employees and criminal penalties. Applied to ISO 9001, clauses 4.2.3, 4.2.4 and 8.0, this title would encourage honesty in records, empower employees and enhance pride of workmanship. It empowers employees by protecting them from fear, being forced to do bad work and retaliation.

**Title IX—white-collar crime penalty enhancements.** Section 906 defines fraudulent accountability as a crime. In ISO 9001, clauses 4.2.3, 4.2.4 and 8.0, it would criminalize dishonest reports and fraudulent quality systems.



When Title IX is combined with other SOX applications to ISO 9000, you might wonder if there would be too great a magnifying glass on top management—creating too great a burden of suspicion. After all, dishonesty in the workplace is not as bad as dishonesty in accounting, is it? Surely, absconding with \$40 million is far worse than cheating on the report of a valve test! Well, if the valve test has a material effect on the cost of quality and we're talking about hundreds of thousands of valves, then yes, dishonesty in the workplace may be as bad as dishonesty in the counting room.

**Title X—corporate tax returns.** This title requires the CEO to sign the corporate income tax. I see no apparent connection of Title X to ISO 9000.

**Title XI—corporate fraud and accountability.** Section 1102 is an extension of Title VIII, covering when records or documents are destroyed or altered to impair an official proceeding. In ISO 9001, clauses 4.2.3, 4.2.4 and 8.0, this title would criminalize the destruction or alteration of quality records to impair an official proceeding. The same argument applies here as in Title VIII and IX—dishonesty is a cost to the customers and shareholders and should have consequences for the miscreant.

## Recommendations

An existing ISO 9000 structure lends itself to integration with a company's financial system, and quality personnel can provide the expertise to help achieve SOX compliance.

Just as SOX makes it necessary for the CEO to understand the financial condition of the company, a SOX based ISO 9001 certification would also make it necessary for the CEO to understand the company quality system. Titles III and IV would require top management to certify compliance of the company quality manual and be accountable for conformance of its quality system.

In today's dynamic global economy, companies are organizing as integrated processes. It is becoming increasingly difficult to separate the notions of production, service, quality and market value. To anticipate an approaching SOX authority, the prudent CEO must know what's going on at all levels in the company.

The following recommendations are easy to do and will assure the CEO of being in control of the company, within the meaning of SOX:

- Set up a financial accounting system con-

formable to ISO 9000.

- Learn the production and service processes. Go to the process managers and business unit managers, and get satisfactory answers to these questions: What is the objective of this process? How do you measure its performance? How do you control this process? How does this operation compare to best practices?

The Sarbanes-Oxley Act is the handwriting on the wall. It has the potential to lead to a new way of doing business, where ethical practices are as important as making money, not because they are a good idea, but because they are the law.

## REFERENCES

1. H. R. 3763, *The Sarbanes-Oxley Act of 2002*, 107th Congress of the United States of America, Washington, DC, Jan. 23, 2002.
2. Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management Framework*, Price-WaterhouseCoopers, 2004 (draft copy).
3. Steve Stanek, "Can ISO Standards Help in Today's Business Climate?" *Knowledge Leader*, Protiviti Corp., April 2, 2004.
4. Joseph M. Juran and Frank Gryna Jr., *Quality Planning and Analysis*, McGraw-Hill, 1980.
5. Organization for Economic Cooperation and Development, *OECD Principles of Corporate Governance*, OECD Publications Service, 2004.
6. *IT Control Objectives for Sarbanes-Oxley*, IT Governance Institute, 2004.
7. Masaaki Imai, *Gemba Kaizen*, McGraw-Hill, 1997.
8. Larry D. Lieberman, "Sarbanes-Oxley Affects Your Private Company Clients," *Wisconsin Lawyer*, June 2004.

**WILLIAM A. STIMSON** is president of SCI Associates, a consulting firm in central Virginia specializing in quality management systems and statistical control. He holds a doctorate in systems engineering from the University of Virginia. The author of *Internal Quality Auditing: Meeting the Challenge of ISO 9000:2000* (Paton Press, 2001), Stimson is presently the chair of ASQ Section 1108 and is a certified quality auditor.

## Please comment

If you would like to comment on this article, please post your remarks on the *Quality Progress* Discussion Board at [www.asq.org](http://www.asq.org), or e-mail them to [editor@asq.org](mailto:editor@asq.org).