

The Sarbanes-Oxley Act: Five Years Later

Corporate America still finds SOX compliance requirements to be burdensome, vague, and frustrating.

John Montaña, J.D.

In 2002, the U.S. Congress passed the Sarbanes-Oxley Act (SOX) with the aim of preventing an assortment of ills related to corporate finance and reporting. The legislation's vehicles for accomplishing its goals were to be a series of steps designed to ensure that publicly traded corporations instituted adequate financial controls, that they documented those controls, and that they certified their accuracy. SOX enforced its goals with a very big stick: personal liability and the possibility of criminal penalties for corporate financial officers.

The Act, which sets only the highest level and most general of requirements but imposes the possibility of substantial penalties for not complying with them, was immediately criticized by corporate America as being overbroad and vague. Those who believed that the gaps left by Congress would be filled in by detailed regulations were disappointed. Regulations adopted by the Securities and Exchange Commission (SEC) offered the same type of vague requirements for an ill-defined but burdensome compliance process rather than substantive guidance on exactly what was to be done.

Lack of Requirements Stymies Compliance

For many corporate compliance personnel, and in particular for those charged with documenting and recording compliance processes, this became a frustrating situation. Compliance regimes common-

At the Core This article

- ▶ Describes the corporate confusion surrounding SOX
- ▶ Discusses subsequent SEC regulations and interpretive guidance
- ▶ Tells why the cost of compliance is so high

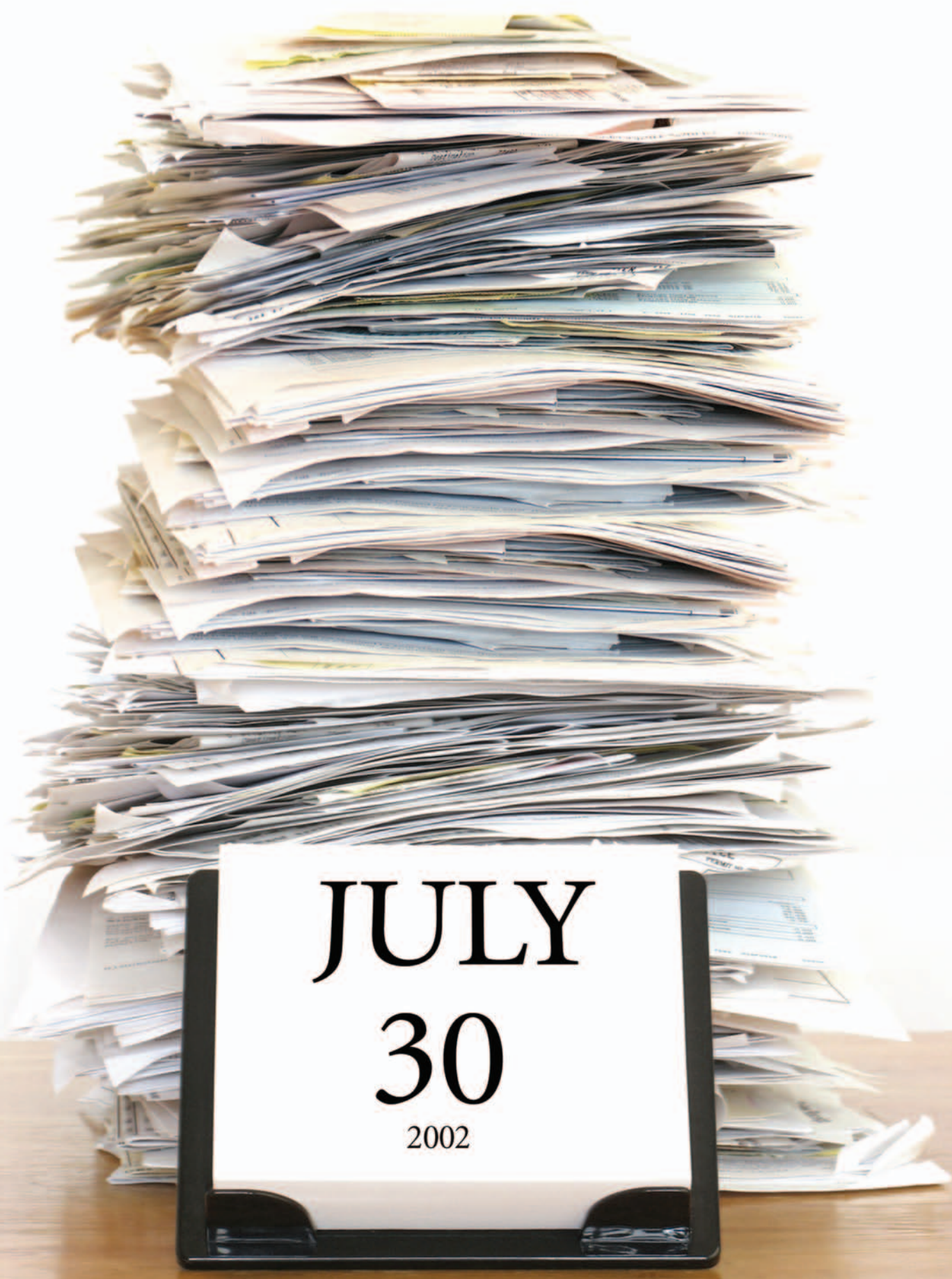
ly impose recordkeeping requirements – often quite detailed and stringent ones. Though many find these requirements to be annoying and burdensome, they do provide a measure of safety. They provide a compliance framework by describing the kinds of records that must be kept, and, by extension, they describe the kinds of processes about which records must be kept and, therefore, about what processes must occur. The end result is records that document

whatever it is that the regulators in question have decided is important and should be recorded.

From the outset, SOX and its regulations were notably devoid of this sort of detailed recordkeeping requirements. The Act itself does not contain any recordkeeping requirements or any records retention periods, with the sole exception of a requirement that accountants maintain audit work papers.

Implementing regulations were little better. For example, they suggest that corporations should maintain “evidential matter” demonstrating compliance. But they do not specify exactly what evidential matter might suffice or what kind of information such matter might contain. And, they do not provide any meaningful standard as to what might constitute an adequate level of substantive compliance.

Consequently, many corporations spent considerable amounts of time, money, and other resources developing SOX compliance manuals, processes for documenting financial controls, and assorted other activities – with little assurance that what they were doing was sufficient or on the mark. Eventually, they settled into whatever pattern of compliance and documentation they



JULY

30

2002

deemed best – generally an exhaustive and intrusive self-audit process with equally exhaustive documentation. They put their faith in believing that subsequent amendments to the Act, its regulations, or interpretive court cases would shed light on the matter before they wound up in court on the question.

SOX Changes

Although it has been five years since SOX was passed, it is worth noting several points before discussing what effect the passage of time has had on it:

First, the full implementation of SOX was delayed two years, meaning that SOX has been in full force and effect only three years.

Second, legislation tends to be around for a long time before its defects are remedied, at least insofar as they are remedied by amending the legislation itself. Regardless of how burdensome businesses may perceive a law to be, its effects must accumulate to the point where a critical mass of the affected community and the general public actively seeks its change. In the legislation business, five years is not a long time at all.

Third, in the intervening years, a number of high-profile events have captured the attention of Congress, corporations, and the public – the Iraq war, a bitterly contested and divisive presidential election, global warming, trade issues, SEC attention to other issues such as backdating of stock options, and a highly partisan atmosphere and series of scandals in the Congress itself – and diverted attention away from SOX.

Consequently, the Act itself remains un-amended. Thus, to the extent that any criticism could be leveled at its provisions five years ago, those criticisms remain valid today.

SEC Regulation Revisions

As for the regulations, the SEC has not promulgated any substantive new SOX rules since March 2004. The rules promulgated up to that time were the

source of much corporate criticism about vagueness, and subsequent rule-making has consisted of fairly minor tinkering with small bits of existing rules. Recent amendments have done little to diminish the vagueness complaint. For example, in the context of financial controls, the SEC has adopted the following definition of “significant deficiency” of a financial control:

“A deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of a registrant’s financial reporting.”

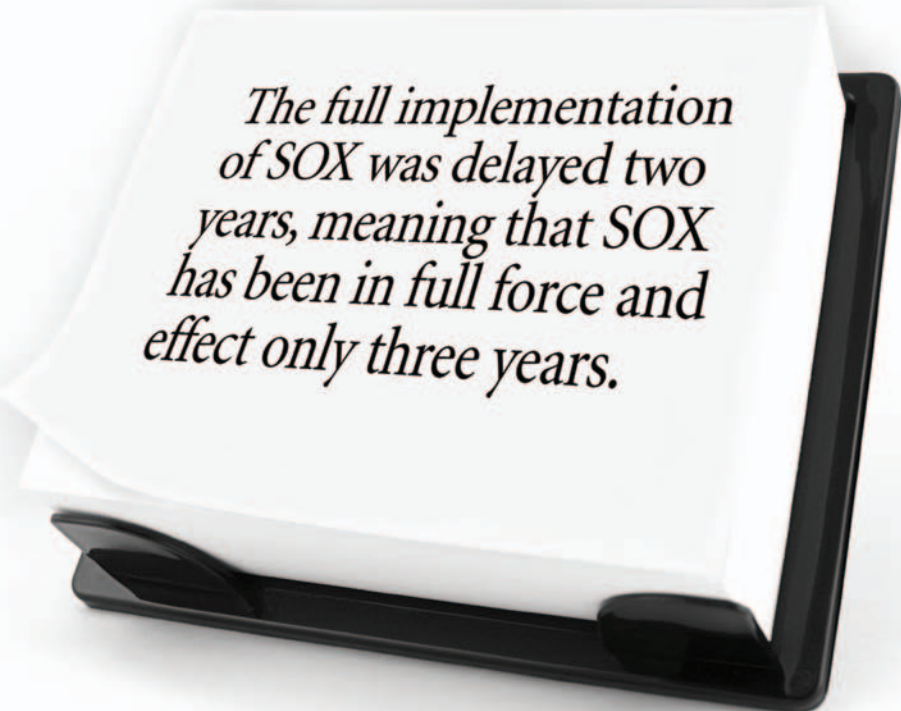
In explaining and defending the definition, the SEC explains: “We believe the definition appropriately emphasizes the communication requirements between management, the audit committee, and independent auditors on those matters that are important enough to merit attention and will allow management to use its judgment to determine the deficiencies that need to be reported to the audit committee and the independent auditor.”

The SEC did not explain, however, how to determine when something is important enough to “merit attention by those responsible.”

A small handful of other such revisions have occurred, such as the revision of rules on management reporting on internal financial controls. The SEC’s approach to compliance in this document is noteworthy. Corporate commentators complained of precisely the vagueness that has plagued SOX from the start – they were looking for, and urged upon the SEC, substantive interpretive guidance that would provide a safe harbor – a course of action presumptive in accordance with the law. The SEC explicitly rejected this approach, stating that “[T]he sufficiency of an evaluation will be determined based on each issuer’s particular facts and circumstances.”

SEC Interpretive Guidance

The SEC has also issued several instances of what it styles “interpretive guidance” wherein, without adopting a rule or mandatory requirement, it attempts to set forth a course of con-



The full implementation of SOX was delayed two years, meaning that SOX has been in full force and effect only three years.

duct it deems reasonable, and which presumably constitutes a course of action that complies with the requirements, such as they are, of substantive regulations. An example of this is the guidance at issue in the rulemaking above. It at last defines, as required by other guidance for several years, the “evidential matter” needed to support internal financial controls reporting, as follows:

“As part of its evaluation of ICFR [Internal Control over Financial Reporting], management must maintain reasonable support for its assessment. Documentation of the design of the controls management has placed in operation to adequately address the financial reporting risks, including the entity-level and other pervasive elements necessary for effective ICFR, is an integral part of the reasonable support. The form and extent of the documentation will vary depending on the size, nature, and complexity of the company. It can take many forms (for example, paper documents, electronic, or other media). Also, the documentation can be presented in a number of ways (for example, policy manuals, process models, flowcharts, job descriptions, documents, internal memorandums, forms, etc). The documentation does not need to include all controls that exist within a process that impacts financial reporting. Rather, the documentation should be focused on those controls that management concludes are adequate to address the financial reporting risks.

In addition to providing support for the assessment of ICFR, documentation of the design of controls also supports other objectives of an effective system of internal control. For example, it serves as evidence that controls within ICFR, including changes to those controls have been identified, are capable of being communicated to those responsible for their performance, and are capable of being monitored by the company.”

This guidance is couched in terms of a philosophy of giving corporations latitude to develop methods of compliance that are suitable to their own resources and situation. In reality, many corpora-

tions believe they are left with no real certainty as to what constitutes compliance with SOX and what records might support that compliance. These corporations must instead await the SEC’s rendering of its judgment on their “particular facts and circumstances” in an individual and undoubtedly adversarial proceeding. Thus, a common theme among the SOX Act’s corporate commentators even today is a demand for more detailed guidance and rulemaking that would provide some certainty.

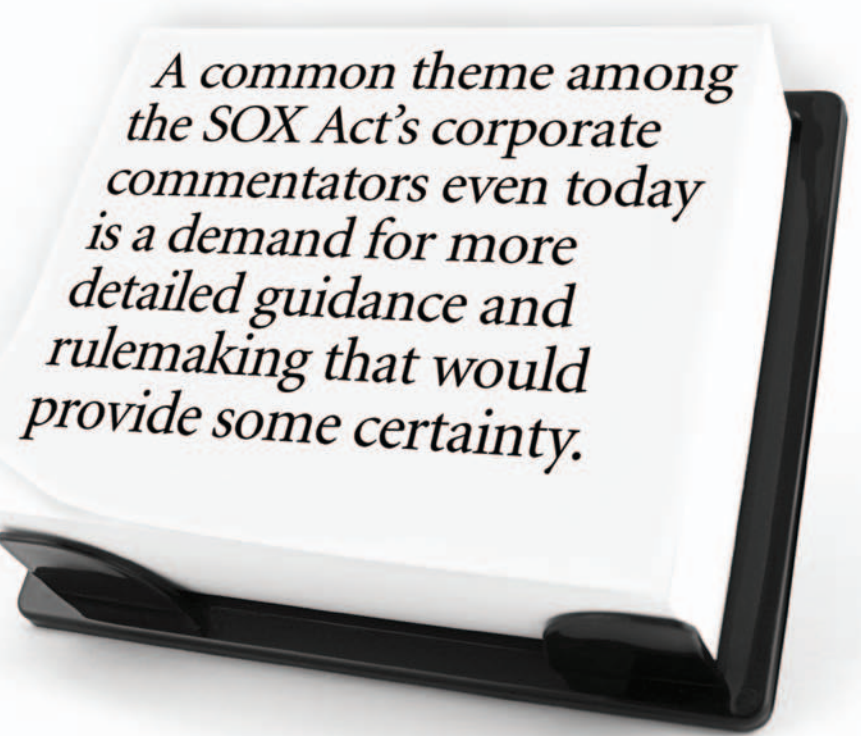
Uncertainty’s High Price

It should be noted here that most corporate commentators do not dispute that SOX, and in particular its section 404 “Management’s Report on Internal Control over Financial Reporting,” are beneficial. At least insofar as they are willing to comment in a public forum, most concede benefits of various kinds in the financial controls and reporting area. Most, however, also complain of high costs. This is not surprising – the lack of certainty necessitates overkill. Corporations do not know where the

line is drawn and must, as a result, make sure they are well past the spot where they believe it to be.

This is also true in the area of records and documentation, the “evidential matter” of SOX terminology. Because the SEC gives only the vaguest of guidance as to what records it expects to see, corporations have no choice but to create exhaustive sets of documentation that in many cases are no doubt far in excess of what the SEC actually expects to see. The alternative is to face the possibility of regulatory actions and lawsuits, both highly intrusive and costly public relations fiascos, or worse, a criminal prosecution; so, the choice is an easy, if expensive one, to make.

However, it may be a misconception to believe that the SEC views its fuzzy approach to section 404 compliance as a license to ignore or give short shrift to the implementation and documentation of financial controls. There has not been a large volume of formal enforcement action, but it is nonetheless there. Notable respondents in SEC enforcement actions for failures in this area



include a case in 2005 against Robert Guccione and *Penthouse* magazine (for boosting its quarterly revenue by improperly reporting a \$1 million up-front payment when the agreement involving the money was actually signed in a subsequent quarter) and a 2004 case involving Cedric Kushner Promotions (for filing a financial report with an official date stamp that preceded the auditors' finalizing their reports).

Only Time Will Tell

So where does SOX stand? Fundamentally, it is in process. SOX is a young law. So far, the SEC refuses to give much in the way of hard rules of compliance, but it continues to hold dialogues with business leaders, the accounting industry, and other interested parties.

Business, for its part, has effectively absorbed or passed along the costs of SOX as a cost of doing business. While many complain about the cost of SOX, no one is as yet unable to meet it. Congress may, at some point, revisit the law, and SEC conversations with business may yet yield more concrete guidance and rules. And

court cases, as yet largely confined to garden variety accounting fraud and similar matters, may yet yield substantive guidance from the courts. In short, corporate

America must wait for this young law to mature. Only then will it be known whether SOX is a swan – or perhaps only an ugly duckling grown old. ■

John C. Montaña, J.D., is a principal of The PelliGroup Inc., a records and information management (RIM) consulting firm. He has authored three books and dozens of articles and is a frequent speaker on a variety of RIM issues, including retention scheduling, legality of information storage media, regulatory compliance, and litigation and discovery. He may be contacted at jcmontana@pelligroup.com.

References

“Penthouse’s Guccione Settles with SEC.” *CFO.com*. Available at www.cfo.com/article.cfm/3597911/c_3597966?f=home_todayinfinance.

U.S. 107th Congress. “Sarbanes-Oxley Act of 2002,” 30 July 2002. Available at www.sec.gov/about/laws/soa2002.pdf.

U.S. Securities and Exchange Commission. “Final Rule: Management’s Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports,” 14 August 2004. Available at www.sec.gov/rules/final/33-8238.htm.

_____. “SEC Charges Cedric Kushner Promotions and Three of its Officers and Directors with Fraud,” 25 March 2004. Available at www.sec.gov/litigation/litreleases/lr18638.htm march 25.