

Meeting the Requirements of Sarbanes-Oxley: The Data Storage Challenge May Not Be So Bad

By Sidney W. Kilgore

INSIDE THIS ISSUE

- 1 Meeting the Requirements of Sarbanes-Oxley: A View from the Storage Perspective
- 1 Welcome to our Compliance Management Newsletter: Your Resource for Information on the Nexus between Business, IT and the Law
- 2 In a Nutshell: The Impact of SOX
- 6 SOX: Where Does IT Fit In?
- 8 For Our International Readers: SOX and Non-U.S. Companies
- 9 Upcoming Topics

Some are already asking when, if ever, the federal government will come down hard on companies for failing to comply with the new regulatory requirements imposed under the Sarbanes-Oxley Act of 2002 – commonly referred to as ‘SarboX’ or ‘SOX’ – by naively suggesting that this legislation may be just another political “dog and pony show” that ultimately will not impact business as forcefully as some have predicted. After all, the argument goes, how many companies actually were prosecuted following the advent of the internal control requirements under the Foreign Corrupt Practices Act (FCPA), which more than a decade ago became a significant factor in motivating company planning for data recovery and security?

Please see *SOX and Storage* on page 2

Welcome to our Compliance Management Newsletter

By Jon William Toigo

“Storage vendors are leveraging fear, uncertainty and doubt to sell “regulatory compliance solutions” that may have nothing to do with regulations themselves.”

Regulatory compliance is being touted by many storage vendors as the key driver of storage purchasing by companies this year. A lot of the marketing around Information Lifecycle Management (ILM) and Data Lifecycle Management (DLM) “solutions,” as inadequate as these are, is founded on a misapprehension of what laws like Graham-Leech-Bliley, Sarbanes-Oxley, and HIPAA actually mean from a storage perspective. Vendors are waging a campaign based on Fear, Uncertainty and Doubt (FUD) to sell their half-baked technology and few seem to notice.

But we do. We asked our legal eagle at Toigo Partners International, who is also one of the most technically savvy guys we know, to pen an article for us that combined his knowledge of law and IT: to set the record straight on regulatory compliance and similar issues.

Please see *Newsletter* on page 9

THE IMPACT OF SOX IN A NUTSHELL

WHO IS AFFECTED?

U.S. and non-U.S. companies.

Companies whose securities are registered under Section 12 of the 1934 Act (public companies), who are required to file reports under Sections 13(a) of 15(d) of the 1934 Act, or who have filed a registration statement under the 1933 Act are subject to SOX.

Even private companies not currently falling within any of these criteria will need to take heed of SOX if they harbor aspirations of launching an IPO one day or otherwise if they may become non-exempt.

Officers and Directors. Among other things, CEOs and CFOs must certify that information contained in company annual and periodic reports fairly represents, in all material respects, the financial condition and results of operation of the company, and can be held personally liable, civilly and criminally, for non-compliance with SOX.

Employees. New whistleblower provisions are intended to insulate employees of a company from retaliation for reporting questionable activities.

Company Securities Lawyers. SOX obligates attorneys to report violations of securities laws or breaches of fiduciary duty to the CEO, general counsel, legal compliance committee, or in some cases, to the Board of Directors of a company.

Continues next page

SOX and Storage from page 1

Such dangerous speculation should not entice company management to retreat from compliance initiatives under SOX, which represents a substantial step in a continuous evolutionary chain of federal regulation of the accountability of public corporations going back more than 70 years. The requirements of SOX are indeed real, and breathe new life and power into the FCPA and a number of other existing laws through the establishment of a comprehensive scheme of certification to ensure the accuracy, integrity, and completeness of the financial information on which investors and regulators must rely, as well as substantial civil and criminal consequences for those who fail to comply, including individual members of corporate management, company counsel, and accountants.

These features make SOX fundamentally different from any previous attempts by the government to prevent corporate corruption and fraud in publicly traded companies. Recent reports suggest that while Treasury Secretary John Snow has expressed concerns about the need for “balance” in enforcement of SOX to obviate criminal prosecutions for mere mistakes, he also has made it clear that in his view, SOX remains important as a reaffirmation of standards of good corporate practice, and that there no need for Congress to amend SOX as originally enacted. SOX therefore represents a new paradigm for corporate governance and operation that is here to stay.

Putting SOX In Historical Context

Since the early 1930s, Congress has sought to codify requirements for controls within organizations, both to control the growth of these organizations and to protect from fraud investors who require accurate information about companies in order to make sound investment decisions. Such legislative initiatives often follow in the wake of a major financial crisis or a series of substantial compliance failures.

For example, concerns about corporate deceit, fraud and misrepresentation in the wake of the stock market crash which heralded the Great Depression gave rise to the Securities Act of 1933 (the 1933 Act) and the Securities Exchange Act of 1934 (the 1934 Act). Together, these laws established standards for the dissemination of information by companies to prospective investors, created the Securities and Exchange Commission (SEC), and formulated reporting requirements with respect to publicly traded securities. The overriding purpose of this regulatory framework was to protect prospective purchasers of publicly traded securities – stocks, bonds, and so forth – by requiring that they be provided with truthful financial and other material information about the securities

Please see *SOX and Storage* on page 3

SOX and Storage from page 2

that, in turn, would allow them to make informed judgments about investments in the company.

The FCPA, first passed in 1977, and subsequently amended in 1988 and 1998, amended the 1934 Act. Intended to stem widespread bribery of foreign officials by U.S. companies – which evidently was interfering with U.S. foreign policy and generally deemed to be a bad thing – the FCPA required management to implement accounting and internal control procedures that accurately and fairly reflected corporate transactions. Although mandating such procedures, the FCPA imposed no clear obligation on the part of company management to ensure the effectiveness of those procedures, which proved a significant loophole in terms of its enforcement.

The passage of SOX in 2002 came on the heels of corporate scandals involving Enron, Worldcom, Tyco, and other huge companies, which exposed the limited effectiveness of existing regulations as a prophylactic measure against fraud, especially when committed by company management, with the aid and comfort of unscrupulous attorneys and accountants. Intended to restore the confidence of investors in publicly traded companies, SOX created a new set of standards actually calculated to prevent fraudulent financial reporting by companies and to improve detection of company fraud when it occurs.

Among other things, SOX effectively amended the internal control provisions imposed under the FCPA by requiring the Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) of certain public companies to certify both the accuracy of the company's books and records, and the internal controls used to produce and verify those books and records. While a number of companies already had documented their internal controls in response to the FCPA through the creation of policy manuals and the like, they typically lacked the documentation necessary for management to evaluate the efficacy of those internal controls in accordance with the certification and disclosure requirements of SOX.

Although the SEC twice in the past had proposed that companies be required to report on the effectiveness of their internal controls and procedures for financial reporting – first in 1979 following the enactment of the FCPA, and again in 1988 following recommendations by the Treadway Commission, an independent private sector initiative created in 1985 to identify the causes of fraudulent financial reporting – neither proposal had come to fruition.

Continued from previous page...

Company Auditors. Firms which perform audits on companies must be registered with an SEC audit review board and must attest to and report on the assessment by management of the efficacy of the internal controls and operating procedures it has established, and face new restrictions on and standards for the services they provide.

Investment Banks and Research Analysts. Enhanced regulations require greater disclosure of actual and potential conflicts of interest.

-SWK

“SOX created a new set of standards actually calculated to prevent fraudulent financial reporting by companies and to improve detection of fraud when it occurs.”

Please see *SOX and Storage* on page 4

SOX and Storage from page 3

Disclosures of the assessment of corporate management as to the effectiveness of company controls, to be made under SOX in accordance with SEC-promulgated rules, could potentially raise the stakes for officers and directors by requiring incidents of fraud or other legal transgressions, e.g., violations of the FCPA to be revealed in company filings with the SEC. This contrasts with the pre-SOX environment, in which the board of directors of a company arguably could have met its obligations to deal with such matters quietly by simply documenting the remedial steps taken by the company in response to the problem, including its internal investigations, the correction of errors in its books and records, and the imposition of appropriate disciplinary procedures on those individuals responsible.

In the new SOX era, then, companies actually may need to consider making advanced voluntary disclosures to the Department of Justice (DOJ) of violations of law and regulations that ultimately will come out in their SEC filings, since under the so-called “qualitative materiality standard” of disclosure for financial statements established by the SEC in Staff Accounting Bulletin No. 99 (dated 12 August 1999), non-disclosure of an FCPA violation, for example, may reflect adversely on the integrity of management. Moreover, such voluntary disclosure may obviate a criminal referral from the SEC to the DOJ as a consequence of the non-disclosure of an FCPA violation in company financial statements.

To further ensure the honesty and integrity of financial statements, and of the certification of those statements by company management, SOX requires public accounting firms performing company audits to evaluate whether the internal control structures and procedures of the company include records that accurately reflect its transactions and disposition of its assets.

This evaluation must include a description of material weaknesses in those internal controls, and a statement of any material noncompliance found during the audit.

In order to conduct a company audit, an accounting firm must first register with the Public Company Accounting Oversight Board (PCAOB). The PCAOB is a five-member body established by SOX to operate under the aegis of the SEC for the purpose of providing oversight of the audit of public companies, establishing audit standards and rules, and inspecting, investigating, and enforcing compliance by the public accounting firms registered with it. Disciplinary or remedial sanctions, or both, may be imposed by the PCAOB on those registered firms and their affiliates in the event of intentional conduct or repeated negligence in carrying out their responsibilities under SOX. Presumably, these requirements will act to stem the opportunity for fraud by precluding the sort of collusion between company management and auditors that occurred in the case of Enron and Arthur Anderson.

So what are the consequences to corporate officers and directors who fail to comply with the new reporting requirements under SOX? They are harsh, to say the least.

For example, Section 906, which establishes criminal liability for the failure of corporate officers to certify properly that the information contained in company financial reports “fairly presents, in all material respects, the financial condition and results of operations of the issuer,” authorizes fines of up to \$1,000,000 and imprisonment for up to 10 years for those officers who certify any statement knowing that the periodic report accompanying the statement does not comport with this requirement.

Please see *SOX and Storage* on page 5

SOX and Storage from page 4

If the violation is deemed to be “willful,” the maximum fine becomes \$5,000,000, and the maximum prison term 20 years. A number of other criminal penalties are substantially enhanced, too.

Penalties for violations of the 1934 Act, for instance, are increased under SOX to a maximum fine of \$25,000,000, and a maximum prison term of 20 years, while penalties for mail and wire fraud expand from a maximum of 5 to 20 years in prison.

On the civil side, in the event a company must restate its accounting due to material non-compliance, SOX requires the CEO and CFO of the company to forfeit bonuses and compensation they have received for a period of one year from the original issue or filing date of the accounting statement which required restatement.

SOX also creates an extension in the statute of limitations applicable to private rights of action for securities fraud, allowing such actions to be filed within 2 years of discovery or 5 years of the first occurrence of the alleged fraudulent event. The failure to take the requirements of SOX seriously carries substantial adverse consequences for the company and for those who run it.

A Key Problem for Data Storage Managers

In a nutshell, compliance with SOX boils down to providing accurate disclosures, on a real-time basis, of any material information which could affect company financial statements through an adequate internal control structure and procedures for financial reporting, the effectiveness of which have been evaluated by management, and confirmed by an independent auditor, who must report on management’s assessment of the effectiveness of the internal controls it has established.

SEC rules to implement the internal control provisions of SOX make it clear that in order to provide reasonable assurance regarding the

reliability of financial reporting, a company’s policies and procedures must:

- 1) include the maintenance of records in reasonable detail, accurately and fairly reflecting the transactions and dispositions of the assets of the company;
- 2) provide reasonable assurance that transactions are recorded as necessary to produce financial statements in accordance with Generally Accepted Accounting Principles (GAAP);
- 3) provide reasonable assurance that no receipts and expenditures of the company are being made without authorization of company management; and
- 4) provide reasonable assurance that any unauthorized acquisition, use, or disposition of the assets of the company that could have a material effect on its financial statements will be prevented or, at least, detected in a timely fashion.

Data storage therefore becomes an integral part of the internal control process. The central problem for data storage managers is to determine, out of the deluge of data a company creates, exactly which information will require special treatment and handling to meet the requirements of SOX. What records are required to “accurately and fairly” reflect the transactions and dispositions of the assets of a company?

SOX Dictates Data Storage Ends, Not Means

Contrary to the views expressed by a host of well-meaning, but legally ill-informed, commentators on the World Wide Web, SOX does not set out any specific requirements for data retention for companies. Rather, SOX

SOX and Storage from page 5

leaves it up to company management to determine what information and records should be kept, and for how long, in conjunction with the establishment and maintenance by management of an adequate control structure and procedures for financial reporting, as required under Section 404.

Whatever management puts in place, however, must meet the goal of providing reliable financial information to investors, and management must provide “reasonable assurance” that it does so.

Essentially, data pertaining to any event – whether financial, operational, or otherwise – that could impact company profit or loss, stock values, or the attainment or failure of business goals, or which would increase or decrease legal exposure or other risk, or which would otherwise materially affect the financial condition of the company, should be retained.

Such data would include not only standard balance sheet and income statement records, but records pertaining to off-balance sheet transactions as well. Account should be taken, too, of data which is not captured electronically if it is required for SOX compliance.

The starting point for assessment is to create an inventory of existing internal control documentation, determine what potential gaps in controls may exist, develop a strategy for closing those gaps, and then implement procedures for validating and capturing the requisite data in real time, or as close to real time as possible. On an ongoing basis, efforts should be made at improving the quality of the data, and reconciling data inconsistencies.

Company management must ultimately make a subjective determination based on reasoned judgment as to what categories of records could be of a material nature. This best may be accomplished in consultation with company auditors, who will eventually be attesting to and reporting on management’s evaluation of its own internal controls.

SOX: WHERE DOES INFORMATION MANAGEMENT FIT IN?

IT will play a central role in assisting management to develop and implement an internal control framework which captures, preserves, and makes available on a real-time basis accurate information regarding all material information which may affect the reliability of the financial statements and reports of a company, and in documenting and evaluating the efficacy of that framework.

The final rule for SOX promulgated by the SEC recommends the use of a model framework for enterprise risk management developed by the Committee of the Sponsoring Organizations of the Treadway Committee (COSO), whose web site is located at www.coso.org.

IT managers may wish to consider integrating the COSO framework with a suitable IT control framework, such as the Control Objectives for Information and Related Technology (COBIT) model developed by the IT Governance Institute and available at www.itgi.org.

Continues Page 7

To illustrate, a hundred e-mail messages between a company employee and a foreign customer that reflect ongoing negotiations leading to a multi-million dollar contract may not have any material bearing on the financial condition of the company at all. On the other hand, they might well become material if they were

Please see *SOX and Storage* on page 7

SOX and Storage from page 6

to reference, for example, a bribe payment in violation of the FCPA.

Again, the idea behind SOX is to achieve financial transparency by ensuring that the records of the company fairly and accurately reflect its business transactions and any dispositions of its assets, and that if fraud occurs, it is prevented, or at least exposed quickly so that prompt remedial action may be taken to mitigate any potential financial impact on the company.

Apart from the decision about what records must be kept, there remains the question of how to treat SOX-required records. A common sense approach is in order here.

- First, the integrity of the records obviously must be protected from unintended alteration or deletion.
- Second, the records must be protected from unauthorized access, so a mechanism for creating detailed audit trails of any interaction involving the records must be implemented.
- Third, since Section 409 of SOX mandates that companies must “disclose to the public on a rapid and current basis such additional information concerning material changes in the financial condition or operations of the [company] ... as the [SEC] determines, by rule, is necessary or useful for the protection of investors and in the public interest,” the records stored should be continuously available in real time to management for reference purposes.

At the end of the day, SOX requires company management to provide a “reasonable assurance” that its financial reporting is reliable, not a guarantee that its financial data are flawless in every respect. What reasonable CEO could argue with the proposition that a company should maintain current and reasonably reliable financial data that accurately and fairly reflect its transactions and any disposition of its assets? What reasonable investor should not be entitled to expect a publicly traded company to do so? Ω

Continued from Page 6...

To address adequately the legal requirements of SOX, IT departments would likely need to consider and evaluate the following critical issues:

- **Reliability.** Procedures must be established to ensure that SOX-required data going into the system is accurate at the time of entry, and that the integrity of the data is preserved and protected from corruption. SOX data may need to be segregated from other data, and may even require its own discrete storage.
- **Security.** Means must be implemented to prevent unauthorized access to, and modification or deletion of SOX data through strong authentication and authorization, as well as alerts and detailed audit trail logs for each and every access or attempt at access.
- **Disaster Recovery.** SOX data must be insulated from catastrophic failure due to Acts of God and other unforeseen events.
- **Real-Time Access and Updating.** Information pertaining to any material event which would impact the financial condition or operations of a company must be captured in real time and made retrievable in real time.
- **Self-Evaluation and Reliability Checking.** Above all, the system must provide means for auditing and enhancing its own performance through an iterative process of assessing, validating, improving, and reconciling SOX data.

–SWK

For Our International Readers: Sox And Non-U.S. Companies

By Sidney W. Kilgore



Non-U.S. companies and their auditors are not exempt from the requirements of SOX. The SEC has stated bluntly, for example, that Section 404, which mandates that every corporate annual report required by either 13(a) or 15(d) of the 1934 Act contain an acknowledgement by management of its responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting, an assessment of the efficacy of that structure and those procedures, as well as an attestation of and report on the same by an independent auditor, “makes no distinction between domestic and foreign issuers and, by its terms, clearly applies to foreign private issuers.” Basically, then, non-U.S. companies who have issued stock on U.S. exchange markets, or who have otherwise registered their securities under the 1934 Act, must begin to compliance as of its first fiscal year ending on or after 15 April 2005, which effectively means 15 July 2005 forward. More than 1300 foreign private issuers from 59 countries were registered with the SEC at the end of 2001.

SOX is merely a recent example of the unfortunate propensity of the United States to exercise extraterritorial jurisdiction – or extraterritoriality – to regulate the activities of non-U.S. companies beyond its own borders. The biggest problem arises when additional regulatory requirements are thrust upon non-U.S. companies regarding matters to which they are already subject to regulation in their home countries, such as the SOX requirement of an independent audit committee, which in civil law countries could unintentionally enhance the power of labor unions because their representatives might be required by their domestic law to sit on the committee and could therefore gain access to sensitive corporate information that could improve its bargaining power in subsequent negotiations.

From a technology standpoint, foreign company compliance with SOX may present special complications. For example, how will implementation of the requirement that companies be capable of providing real-time disclosure of material changes in their financial conditions or operations be affected by a presence in multiple time zones? To what extent will linguistic differences in documentation impact such a requirement? What additional steps may be necessary to meet the rule that foreign accounting standards be referenced to the most directly related provision of Generally Accepted Accounting Principles (GAAP), the U.S. standard for accounting?

All good questions that remain to be answered. Ω

Newsletter from page 1

The article became a newsletter. And the newsletter evolved into an important and valued component of TPI's informational service offerings.

Going forward, Mr. Kilgore will expand his subject matter to include the legal issues affecting data managers everywhere, from matters of intellectual property rights to matters of personal privacy. And of course, he will continue to monitor the nexus between regulatory developments and IT.

Each issue will be a sort of "legal briefing" in layman's terms. While not a substitute for legal advice, by any means, Kilgore's commentary will provide the reader with enough background to make better use of their consultations with legal professionals.

The Compliance and Management Newsletter does not accept vendor advertisement. Instead, we will seek to cover our costs for bi-monthly publication through reader subscriptions of only \$600 per year or \$100 per issue.

Those readers who elect to join our on-line communities, IT-Sense (www.it-sense.org) for IT decision makers or the Data Management Institute (www.datainstitute.org) for data managers, will receive a discounted subscription to the Newsletter as a member benefit. Membership also provides access to a wealth of other information resources including white papers and other specialty newsletters covering data management, legal matters pertaining to storage, disaster recovery planning, information security, and other useful topics.

We welcome you to visit our sites today and learn more about the benefits of membership.

**Toigo Partners International
Data Management Institute**

1538 Patricia Avenue
Dunedin, FL 34698 USA
Phone: +1.727.736.5367
Fax: +1.727.736.8353

E-mail: info@toigopartners.com



Compliance & Management: Timely And Accessible Legal Briefings That Busy Information Managers Will Find Valuable

Everyone understands that knowledge is power. As an IT professional, however, when do you have time to keep up with legal developments that impact your business? Could you be out of compliance with some new law or regulation of which you aren't even aware? Are there inexpensive ways for you to minimize your company's legal exposure from dangers you know little or nothing about? Do profitable opportunities exist that you aren't taking advantage of simply because you don't understand the legal avenues necessary to seize on those opportunities?

Every other month, this newsletter will explore legal topics specially selected to help you fill in these gaps. Written in concise and clear language you will appreciate, the articles you will find in these pages will help to expand your grasp of even relatively arcane legal subjects, and enable you to be more proactive and effective in protecting your business and finding an inside track to greater success. Forthcoming issues will cover the following topics:

- Alternative Strategies for Vendor Sharing of Proprietary Technology for Mutual Benefit
- Limits of Employee Privacy in the Use of the Computational Resources of an Employer
- Status of Electronic Contracting in Commercial Transactions
- Jurisdictional Issues In TransBorder Flows of Information
- Deciding Whether To Patent

We invite you, the reader, to suggest additional topics that would be of value to you. Email us at info@toigopartners.com.

The Compliance and Management Newsletter is a bi-monthly publication of Toigo Partners International and the Data Management Institute. All content of this publication is Copyright © 2005 by Toigo Partners International LLC and Sidney W. Kilgore. All rights are reserved.