

The Sarbanes-Oxley Act

Understanding the Implications for Information and Records Management

I. Introduction

Randolph Kahn, ESQ.
Barclay T. Blair

The Sarbanes-Oxley Act of 2002 (“SOX”)² is a complex piece of legislation that was passed in the wake of the numerous high-profile corporate scandals that have filled the headlines over the past few years. Although SOX was signed into law many months ago, its full impact on business practices has yet to be felt. The reforms it makes to existing laws are broad, and its new provisions are sweeping. While some of the SOX provisions are in full force and effect, some of its provisions have yet to be phased in.

What is clear is that many companies are making major changes – and spending a great deal of money – to bring their organizations into compliance with SOX. A recent survey of public company executives found that 91% had already started to make changes to compliance practices as a result of SOX, but a majority thinks that SOX compliance will cost more than they initially expected.³ Many studies estimating the costs of SOX compliance have been done, with one recent analysis pegging the cost of compliance in the billions for public corporations, with the average first-year cost per company at \$500,000.⁴

The first charges against a company and its executives under the certification requirements of SOX have already been filed and settled,⁵ and a public company auditor has already been arrested and charged under SOX for allegedly altering and destroying audit documents.⁶ The SEC, for its part, filed nearly 50% more “financial fraud and reporting cases” in fiscal 2002 than in the previous year.⁷

“And today I sign the most far-reaching reforms of American business practices since the time of Franklin Delano Roosevelt. This new law sends very clear messages that all concerned must heed. This law says to every dishonest corporate leader: you will be exposed and punished; the era of low standards and false profits is over; no boardroom in America is above or beyond the law.”

US President George W. Bush, signing the Sarbanes-Oxley Act July 30, 2002¹

While a great deal of the coverage and discussion regarding SOX has rightly focused on its immediate impact on accounting practices, financial reporting, and corporate governance, the impact of the law is not limited to these areas. In fact, the law reaches right to the core of a company by directly impacting the way that companies must retain, control, manage, and use the lifeblood of their organization – namely, their information assets. Like information and records management, SOX compliance is an ongoing process that requires a “top-to-bottom” approach and constant vigilance on the part of those responsible for ensuring compliance. In fact, under SOX, companies are expected to routinely report on their compliance and to identify, on an on-going basis, any problems found with their procedures.

Not a legal opinion or legal advice. For all questions regarding SOX and SEC regulations seek legal counsel.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

At its core, SOX is an attempt to improve the accountability and transparency of public companies. Accountability and transparency depend upon trustworthy and accurate business records. In essence, business records serve as the bedrock of accounting and financial reporting systems. Earnings figures, for example, do not materialize from thin air - rather they derive from documentation of business transactions - invoices, purchase orders, contracts, payment information, and so on. Obviously, if these records are inaccurate, so too will be the information in the accounting system. As such, compliance with SOX relies on a foundation of information and records management practices that ensure the trustworthiness and accuracy of business records.

It is critical then, that companies understand how SOX impacts information and records management practices. This report examines the impact of SOX on this area and explores ways that companies might address SOX in their own information and records management programs.

WHERE LAW & TECHNOLOGY MEET



II. The Post-Sarbanes-Oxley Business Era

Although SOX is targeted at public companies and their auditors,⁸ all organizations - not just public companies - should assess their information and records management practices in the context of the passage of SOX and the events of the last few years. SOX became law in large part because elected officials believed that current laws were insufficient to protect the investing public and the public was demanding that the government take action to prevent future corporate wrongdoing and to punish wrongdoers. Moreover, SOX was only one part of the government's strategy for addressing these issues. For example, the President's Corporate Fraud Task Force, created around the same time as SOX, has a mandate to "aggressively investigate and prosecute fraud," and has aided in obtaining "over 250 corporate fraud convictions or guilty pleas."⁹

Although some may disagree with the approach taken by SOX, it would be hard not to agree that the post-SOX era is one characterized by heightened scrutiny of all organization's internal practices. In addition, many of the high-profile cases (Enron/Andersen, for example) that influenced the passage of SOX specifically involved allegations of business record destruction and alteration – thereby connecting issues of corporate fraud and records management in the mind of shareholders, corporate boards, and the public at large.

In fact, on the subject of business records destruction, Section 802 of SOX updates the criminal code to provide stiffer criminal penalties for individuals who destroy information "with the intent to impede, obstruct, or influence the investigation or proper administration of **any matter** within the jurisdiction of any department or agency of the United States." (emphasis added)¹⁰ Arguably, the scope of this language suggests that SOX Section 802 criminal penalties apply to activities beyond a bankruptcy court filing, or government investigations and impact organizations beyond just public companies. Section 802 is discussed in greater detail below.

The net result is that in the post SOX-era there is arguably greater awareness than ever before of information and records management issues. As such, all organizations – not just public companies – should revisit their records management programs to ensure that they adequately address their business, operational, legal and compliance needs. Indeed, private companies not directly affected by SOX have chosen to adopt SOX as a template for their internal accounting, governance, and information and records management practices. In any case, such a review needs to begin with the realization that a consistent and effective approach to managing records not only is essential to gaining and keeping the trust of customers, regulators, partners and other parties, but also is essential to business success as a whole in the post-SOX era.

Three fundamental issues that organizations must consider in conducting such a review include:

- 1) **Information and records management policies and procedures.** Information and records management policies and procedures should be regularly reviewed, but there is no time like the present to ensure that these tools are up-to-date and reflect the organization's current operational structure, legal and regulatory environment, litigation history, and business goals.
- 2) **Leadership support and organizational structure.** The importance of information and records management programs should be reflected in their visibility and high-level support. This is accomplished in large part by senior executives taking an active role in the development, management, and promotion of the programs throughout the company. In addition, senior leadership must regularly make clear to all employees the importance of the program and compliance with its directives. Finally, organizations need to ensure that the programs are adequately funded

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

and staffed with personnel who have the right experience and trained to ensure program success.

- 3) **Technological environment.** An increasing number of information and records management failures derive from inadequate investment in – and management of – information technology used for creating, retaining, and managing business records. This trend is not likely to reverse itself as organization's dependence on digital information only continues to grow and the mismanagement of email and other forms of digital information only provides a growing target for litigators and regulators. Organizations must ensure that their deep reliance on information technology is matched by their commitment to ensuring that records in digital form are managed with the same care and attention as records in paper form.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

III. SOX Recordkeeping Obligations

Aside from the general impact that SOX has on the role and profile of information and records management practices, SOX also has a direct impact on the types of information that must be retained by companies and the length of time that this information must be retained.

Retention of Audit Information

Before SOX, public company auditors often only retained final and official documentation that directly supported their audit conclusions. SOX Section 802, and related SEC regulations, now require auditors to retain a broader scope of audit-related information, and retain certain information for 7 years, perhaps longer than prior to SOX.¹²

“The availability of documents under this rule will assist in the oversight and quality of audits of an issuer’s financial statements. Increased retention of identified records also may provide critical evidence of financial reporting impropriety or deficiencies in the audit process.”

The scope of information that must be retained by public company auditors under the new regulations is potentially very broad, and includes, “records relevant to the audit or review, including workpapers and other documents that form the basis of the audit or review, and memoranda, correspondence, communications, other documents, and records (including electronic records).”¹³ The SEC has stated that there are two criteria that should be used for determining whether or not specific information must be retained:

SEC Release No. 33-8180, “Retention of Records Relevant to Audits and Reviews”¹¹

- 1) It was “created, sent or received in connection with the audit or review, and”
- 2) It contains “conclusions, opinions, analyses, or financial data related to the audit or review.”¹⁴

Clearly, these SOX record retention requirements require auditors to revisit existing records retention policies and schedules. In addition, information falling within these requirements may exist in many different forms, including e-mail messages and other types of digital communications. Also, the information may reside in many different physical locations, from central servers to auditor’s handheld devices. Furthermore, even though the SEC has stated that information such as drafts, duplicates, copies of documents that have been corrected, and voicemail messages, “generally would not fall” within the retention requirement, this is only true if those documents do not contain information “relating to a significant matter” that is “inconsistent with the auditor’s final conclusions.”¹⁵

New Record Categories

SOX also creates several new types of records that must be retained and properly managed. Specific examples of these new record categories include:

- **Website records.** Sections 403 (and the related SEC regulation) require companies that have a corporate website, to post within a specified time, a statement regarding certain major changes in the ownership of stock.¹⁶ Therefore, companies will need to be able to retain and manage adequate documentation of this posting, including the information that was posted, when it was posted, and where on the website it was available.
- **Internal control reports.** The “internal control reports” required by Section 404 and the executive certifications required by Section 302 (explained in detail below) are in and of

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

themselves records that must be properly retained and managed.¹⁷ The process used to create these documents is also likely to produce a variety of information that companies will likely want to retain and manage as records in order to substantiate the conclusions contained in the reports and certifications.

- **Complaints.** Section 301 requires a company's audit committee to establish "procedures for . . . the receipt, retention, and treatment of complaints" received from employees regarding accounting and auditing practices. Employees must be able to submit such complaints anonymously, but as the law makes clear, records of these complaints must be retained. In addition, it may be necessary to retain records showing that the process has been developed and implemented, and demonstrating how various complaints received through the system were addressed.¹⁸

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

IV. SOX Internal Controls: The Bridge Between Accounting, Corporate governance and Records Management

SOX is a complex law that makes numerous changes to existing laws and regulations, and creates many new legal obligations. Many of these changes have no direct relevance to information and records management and address issues specific to the public accounting profession. As a practical matter, SOX required the SEC to amend and add to several of its existing rules and regulations.¹⁹ As such, much of the law's impact is felt through the SEC's regulations.

The concept of "internal controls" is central to SOX, and it has a direct bearing on information and records management. Section 404 of SOX (which becomes effective June 15, 2004 for many companies) requires senior management to include an "internal control report" that assesses the effectiveness of their "internal controls and procedures . . . for financial reporting" in each annual report.²⁰ Section 404 also requires a company's auditor to "attest to and report on" this report - to, in effect 'assess the assessment.' Another section of SOX, Section 302 (already effective)²¹, requires CEOs and CFOs to certify in their annual and quarterly reports that they are responsible for these internal controls, and Section 906 (already effective) provides criminal penalties including fines and jail terms of up to \$5,000,000 and 20 years, respectively for executives who certify false financial reports.²² SOX required the SEC to create detailed regulations regarding these procedures, which it did in June 2003.²³

Although the central SOX concept of "internal controls" is well-known in the public accounting world, it is less common in the information and records management world. However, in the post-SOX era, information and records management professionals need to become intimately familiar with this concept, as it has a direct bearing on records management within corporations, and provides a conceptual bridge between accounting, corporate governance and records management.

Defining "internal controls"

When the SEC promulgated its final SOX regulations, it noted that there was some confusion about the precise meaning of the term "internal controls," even within the accounting profession:

" . . . there has been some confusion over the exact meaning and scope of the term 'internal control,' because the definition of the term has evolved over time. . . . Historically, the term 'internal control' was applied almost exclusively within the accounting profession . . . From the outset, it was recognized that internal control is a broad concept that extends beyond the accounting functions of a company."²⁴

In any case, the SEC's final definition of internal controls makes clear that SOX internal controls have a scope that impacts information and records management practices.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

Internal Controls in Information & Records Management

*“The term ‘internal control’ over financial reporting is defined as a process designed by, or under the supervision of [the company’s senior executives] and effected by the [company’s] board of directors, management and other personnel, to provide reasonable assurance **regarding the reliability of financial reporting** and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:*

- 1. **Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect** the transactions and dispositions of the assets of the issuer;*
- 2. **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*
- 3. Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer’s assets that could have a material effect on the financial statements.”*

*Exchange Act 13a-15(f)
(emphasis added in bold throughout)*

As the SEC definition makes clear, internal controls include policies and procedures designed to ensure that records are maintained in a way that “accurately and fairly reflect” the business transactions of a company, and “provide reasonable assurance that transactions are recorded as necessary” to support accurate financial reporting and good corporate governance.

Although there are a number of public accounting techniques and tools that are used as “internal controls,” arguably information and records management policies, technologies and programs are also a critical form of internal control that companies need to employ in order to have comfort with their Section 404 “internal control report,” statements and their Section 302 certifications. After all, information and records management programs are explicitly designed to ensure the accuracy and trustworthiness of records that document business transactions and activities.

How can an executive comfortably certify a financial report if he/she does not have assurances that the storage and archiving systems responsible for retaining, managing, and producing the data upon which those financial reports are based are properly configured and managed? A fundamental reason to retain and manage business records in the first place has always been to support and document business decision-making and strategy. Under SOX, this reasoning is more relevant than ever before.

In the wake of SOX, companies must ensure that (specific definitions aside) their approach to managing business records is an approach that supports their SOX needs. In other words, information and records management practices must be sufficiently designed, implemented, enforced, and audited to ensure that they support the company’s need for accurate financial information. They must be sufficient to give executives comfort that the information that they are certifying as required by SOX is accurate, trustworthy, and can be substantiated by the company’s own business records.

WHERE LAW & TECHNOLOGY MEET



V. Protecting the Crown Jewels: Destruction & Alteration of Business Records

As explored in the previous section, SOX is specifically designed to ensure that a company's reported financial information can be relied on - and requires companies to invest in procedures that ensure information is recorded and managed in a trustworthy manner. However, SOX does not stop there. In fact, Section 802 – one of the most arresting sections of SOX – outlines dramatic criminal penalties for the improper destruction or alteration of business records. In doing so, SOX recognizes that reliable and accurate financial reporting depends on protecting the crown jewels – the records, documents and other evidence that supports, documents, and provides the foundation for that financial information.

“Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.”

Sarbanes-Oxley Section 802 (emphasis added)

When “Normal” Practices No Longer Apply

Contemporary information and records management practices are often based on a “lifecycle” approach. In this model, each business record has a lifecycle that begins when it is created, and ends when the records is no longer required for business, operational, legal, compliance or other purposes. In this sense, the disposition of business records is as integral a part of information and records management as is the act of retention. Disposition of business records according to a documented policy and schedule allows companies to purge unnecessary information that is costly to store and manage – without fear of running afoul of the courts or regulators.

However, companies also have an obligation to suspend normal disposition practices in the face of anticipated or ongoing audits, investigations, litigation, and other formal proceedings. Although this obligation existed long before the passage of SOX, the increased criminal penalties provided by Section 802 of SOX for failing to meet this obligation warrant renewed focus on this issue.

Companies need to have a mechanism in place, often called a (Records Hold or Legal Hold) to inform executives and employees affected by the anticipated or ongoing audit, investigation or litigation of their obligation to preserve (and possibly produce) specific information. Specific considerations for this mechanism include:

- **Take action at the first sign of trouble.** An obligation to preserve information may begin the moment that a company has reason to believe that it may become involved in an investigation or litigation. Do not wait for a subpoena or other formal request for information before taking action to preserve relevant information. Also, do not assume that the obligation to preserve is limited to court proceedings. Section 802 provides a very broad definition of the proceedings that it applies to: “**any matter** within the jurisdiction of **any department or agency** of the United States or any case filed under title 11, or **in relation to or contemplation of any such matter or case.**”
- **Identify the recipients and the subject matter.** It is important that the right people receive notification of the need to preserve information, and that they are provided with specific direction on the kinds of information that must be preserved.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

- **Include all forms of information.** Preservation should include all information in tangible form, including e-mail messages and other forms of digital information and records.
- **Document the policy.** Create formal written policies and procedures outlining the preservation process and identifying the specific tasks and roles within the process. Manage that documentation as business record.
- **Retain notices.** Retain e-mail memos, forms, and other information used to disseminate information about the need to preserve information and manage that as a business record.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

157 LEONARD WOOD NORTH • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

VI. The Role of Information Technology in SOX Information & Records Management Compliance

Clearly, in today's business environment, where the vast majority of information created, received, and used by companies is in digital form, SOX compliance must be supported by the capabilities, configuration, and management of a company's information systems. As such, companies should ensure that the information systems they use to retain, store and manage business records support SOX compliance requirements, including:

- **Information protection.** Employ "fine-grained" access controls and protection against unauthorized or inadvertent alteration, destruction, or corruption of business records and financial information.
- **Audit trails.** The ability to accurately track and provide an "audit trail" of all interactions with systems housing critical records and information. Information and records and document management software and hardware and secure storage environments form a critical "internal control" that provides a company with assurances that its financial and business information is accurate and reliable. The ability to demonstrate and document this reliability is central to Section 404 and 302 requirements.
- **Longevity.** Ensure that the archiving and storage systems and media used to retain required records will support long-term, reliable access. Under Section 802, a failure to provide information sought by investigators because of obsolete, unsupported, or incompatible software and hardware is unlikely to provide an adequate defense. In the electronic world making information "unavailable" may have the same affect as "shredding."
- **Support for policies and procedures.** Information and records management software and hardware should be designed in such a way that it can be easily configured to meet policy directives. As SOX illustrates, the kinds of information that must be retained, and the length of time that it must be retained, may change as new laws and regulations are passed, and as a company grows and changes.

WHERE LAW & TECHNOLOGY MEET



VII. Conclusion

The era of Sarbanes-Oxley is upon us. While its impact has already been widely felt, SOX will likely have a substantial on-going impact as public companies seek to build and maintain compliant systems. SOX has and will continue to have a direct impact on the role and profile of information and records management within public corporations and beyond. Executives need to view their records management program as a critical “internal control” that will help them ensure that they meet SOX requirements for the accuracy and reliability of financial reporting. SOX planning should therefore include a review of existing information and records management policies, technology, funding, staffing, and organizational structure. At the same time, the relationship between the IT/IS and Records Management department should be examined to ensure that it reflects the depth of the company’s reliance on IT for critical and sensitive business transactions. Business records must be protected from unauthorized alteration, corruption and destruction at all times - a requirement that takes on even greater significance when a company anticipates or is involved in audits, investigations, litigation, or other formal proceedings. Companies must have a clear mechanism to ensure that the right people throughout the organizations are informed of their obligation to preserve business records and other information when this occurs.

In the end, SOX is a mandated corporate governance process – one where a company’s existence, financial health and individual accountability and responsibility will be challenged like never before. At the center of this new governance model are company records. Failing to properly manage them can have – and has had – devastating consequences.

VIII. About Kahn Consulting

Kahn Consulting, Inc. (“KCI”), headed by founder and principal Randolph A. Kahn, Esq., is a consulting firm specializing in the legal and policy issues of information technology. Through a range of services including information management program development, risk management audits, policy development and evaluation, product assessments, legal and compliance research, and education and training, KCI helps its clients address today’s critical issues in an ever-changing regulatory and technological environment. Based in Chicago, KCI provides its services to Fortune 500 companies and state and federal governmental agencies in North America and around the world. Kahn has advised clients such as McDonalds’ Corp., Hewlett-Packard, United Health Group, the Federal Reserve Banks, Ameritech/SBC Communications, Motorola, Merck and Co., Mutual of Omaha, and the Environmental Protection Agency. More information about KCI, its services and its clients can be found online at: www.KahnConsultingInc.com.

IX. Endnotes

¹ “President Bush Signs Corporate Corruption Bill,” White House Office of the Press Secretary, July 30, 2002. Online at: <http://www.whitehouse.gov/news/releases/2002/07/20020730.html>

² Pub. L. 107-204, 116 Stat. 745 (2002).

³ “Senior Executives Less Favorable On Sarbanes-Oxley, PricewaterhouseCoopers Finds,” PricewaterhouseCoopers Management Barometer, July 23, 2003.

⁴ “Sticker Shock,” Alix Nyberg, CFO Magazine, September 08, 2003.

WHERE LAW & TECHNOLOGY MEET



⁵ "Poultry firm settles first Sarbanes-Oxley charge," Reuters, August 18, 2003.

⁶ "Former Ernst & Young Audit Partner Arrested for Obstruction Charges and Criminal Violations of Sarbanes-Oxley Act," US Department of Justice press release, September 25, 2003.

⁷ "President's Corporate Fraud Task Force Compiles Strong Record," White House Office of the Press Secretary Fact Sheet, July 22, 2003. Online, <http://www.whitehouse.gov/news/releases/2003/07/20030722.html>

⁸ The term "public company" is used broadly here to include a range of entities that come under the SEC's jurisdiction. There may be cases where private companies are affected, such as when they have a public bond offering, for example.

⁹ "President's Corporate Fraud Task Force Compiles Strong Record," White House Office of the Press Secretary Fact Sheet, July 22, 2003. Online, <http://www.whitehouse.gov/news/releases/2003/07/20030722.html>

¹⁰ Pub. L. 107-204, 116 Stat. 745 (2002), Section 802.

¹¹ SEC Release No. 33-8180, "Retention of Records Relevant to Audits and Reviews," January 24, 2003.

¹² The compliance date for the SEC Regulation (Regulation S-X) implementing this part of SOX Section 802 is October 31, 2003.

¹³ SEC Release No. 33-8180, "Retention of Records Relevant to Audits and Reviews," January 24, 2003 (hereafter SEC Release No. 33-8180).

¹⁴ SEC Release No. 33-8180.

¹⁵ SEC Release No. 33-8180.

¹⁶ SEC Release No. 33-8230, "Mandated Electronic Filing and Website Posting for Forms 3, 4, and 5," May 7, 2003.

¹⁷ SEC Release No. 33-8328, "Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," June 5, 2003.

¹⁸ Pub. L. 107-204, 116 Stat. 745 (2002), SEC. 301.

¹⁹ Including, for example, Regulation S-K, S-B, S-X, and Exchange Act Rules 13a-14, 13a-15, 15d-14 and 15d-15.

²⁰ Pub. L. 107-204, 116 Stat. 745 (2002), SEC. 404.

²¹ Pub. L. 107-204, 116 Stat. 745 (2002), SEC. 302.

²² Pub. L. 107-204, 116 Stat. 745 (2002), SEC. 906.

²³ SEC Release No. 33-8328, "Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," June 5, 2003.

²⁴ SEC Release No. 33-8328, "Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," June 5, 2003.

WHERE LAW & TECHNOLOGY MEET

