
Darning SOX:

Technology and Corporate Governance Elements of Sarbanes-Oxley

page 2	Introduction
page 3	Patching the Holes: Internal Controls and Information Technology
page 6	Hoping the Patches Hold: Ongoing Evaluation of Internal Controls
page 6	Showing Holes in Your SOX Compliance: Disclosure
page 7	The Stigma of Bad SOX Compliance: Responsibility, Penalties, Enforcement and Deadlines
page 10	Conclusion: Keeping up your SOX Compliance

Introduction

The process of “darning a sock” is probably not an experience that most people in today’s society have had. In generations past, however, it was not uncommon to “darn” a sock (seal a hole in it) by weaving thread over the hole or tacking on new fabric. Luckily, more durable fabrics and cheap textiles have largely consigned this experience to the chapters of history. The origin of the term “darn” is unknown, but a plausible explanation is that the word was uttered by persons who had to perform this tedious task and were simply too polite to say “damn.”

Today, an entirely new generation of businesspeople may be using the word “darn” (or more colorful terms) as they face a new type of SOX: the Sarbanes-Oxley Act. SOX also attempts to mend a number of holes, not in fabrics, but in a lack of corporate controls over financial reporting, disclosure and auditing that led to corporate scandals involving the manipulation of financial information to boost share value.

SOX requires publicly held companies to implement internal controls over their financial reporting, operations and assets, to evaluate the strengths and weaknesses of these internal controls in official documents filed with the SEC and to make regular disclosures concerning the viability of these controls and potential fraud or losses that may affect the company’s financial position. Because most companies’ financial reporting and operations depend heavily on information technology, and because many corporate assets now exist in the form of critical data, SOX has significant information security implications for companies governed by the law.

Although SOX includes wide-ranging provisions relating to numerous aspects of corporate transparency, this paper will focus on three elements of the law that may have the greatest ramifications for information technology and which appear in Sections 302, 404 and 409 of SOX (and corresponding SEC Rules and Regulations). These elements are:

- Control (internal controls)
- Evaluation (governance, measurement and recordkeeping), and
- Disclosure (reporting and certification)

These “control, evaluate and disclose” elements are not stand alone requirements, and must work together as pieces of an overall SOX compliance process. Companies that are required to comply with the law must adopt changes to corporate governance and a process of change auditing to adequately meet the challenges of SOX compliance.

¹ Daniel J. Langin is the principal of Daniel J. Langin, Attorney at Law, LLC. He has over 16 years of experience in private and corporate practice, including ten years of experience in technology, insurance coverage and intellectual property litigation and counseling. For more information, see www.langinlaw.com or contact Daniel at (913) 661-2430 or dlangin@langinlaw.com. This article is provided for general educational and informational purposes. It is not intended to provide legal advice.

Patching the Holes: Internal Controls and Information Technology

Perhaps the most talked-about requirements of SOX are the ones related to internal control over financial reporting. Section 302 of SOX and the SEC Regulations that were passed to implement it require corporations to adopt internal controls over financial reporting and operations. Specifically, sections 302(a)(4)(A) and (B) of SOX require a company's chief financial officer and chief executive to certify in quarterly and annual reports to the SEC that they:

- (A) are responsible for establishing and maintaining internal controls;
- (B) have designed such internal controls to ensure that material information [about the company and its subsidiaries] is made known to such officers by others within those entities²...

Although this sounds complicated, it boils down to creating a process to ensure that top management gets truthful information about the company's finances and operations from subordinates and reports it to the SEC. The goals are: (a) to make sure that financial results reported to shareholders are accurate, and; (b) to prevent top management from placing the blame on subordinates or breakdowns in procedures not directly under their control.

The term "internal control" holds several layers of meaning. It is first and foremost defined in the final SEC Rules implementing SOX as:

A process designed by, or under the supervision of, the registrant's principal executive and principal financial officers... to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with [GAAP] and includes those policies and procedures that:

- (1) Pertain to the maintenance of records that... accurately and fairly reflect the transactions and dispositions of the assets of the registrant;
- (2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with [GAAP], and that receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant; and
- (3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements³.

Each of the three elements of this definition of "internal controls" impacts information technology. For the first element (maintenance of records), companies must adopt policies and procedures to ensure that electronic records of transactions and asset disposition are kept and not later corrupted. Keys to this requirement are document retention policies and technologies that detect changes and can restore records to a last known correct state. The first step in the process may be very difficult: according to a 2003 survey by the Hackett Group, 47% of the companies surveyed used individual spreadsheets for planning and budgeting. Combining all of this individual information into one financial reporting database will be challenging for many companies.

² Sarbanes Oxley Act Section 302(A)(4)(A) & (B).

³ Exchange Act Rules 13a-14(d) and 15d-14(d).

The second element presents an equally daunting task. The purpose of it (ensuring that transactions are duly recorded and receipts and expenditures duly authorized) is to prevent the kind of “off-books transactions” and manipulation of revenue recognition (such as channel stuffing) that has characterized many corporate violations of SEC Rules. The steps required to implement this element of internal controls involves not only internal process changes (such as requiring supervisor authorization of expenses), but also information security controls over the recording and authorization aspects of this step that involve information technology.

The third element perhaps most clearly involves information security. Policies and procedures, and tools, for the “prevention or timely detection of unauthorized acquisition, use or disposition of... assets” are at the heart of any reasonable information security program. Because much of a company’s assets lie in its information assets, this requirement translates into information security controls that will prevent or detect the unauthorized acquisition, use or disposition of information or other assets that may affect the company’s bottom line. Information such as customer lists, product development plans and trade secrets clearly fit the bill as assets which, if lost, could materially affect the financial condition of a company.

Standards for applying these three elements of internal controls, however, are not more specifically defined within SOX. Instead, regulated parties need to refer to other sources for more detailed standards. Two standards that are frequently cited in internal controls discussions are COSO (Committee of the Sponsoring Organizations, Treadway Commission) and COBIT (Control Objectives for Information and related Technology) created by the Information Technology Governance Institute, or “ITGI”).

SEC commentary to the SOX Regs refers to standards as the basis for the term “internal controls” under Sections 302 and 404 of SOX. COSO is made up of five components (Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring). Although several of these components sound very much like information technology control components, COSO is an accounting standard, not an information technology standard. It focuses on reporting and operations-based controls for the accounting process, not information security processes. One commentator succinctly summarized the disconnect between COSO and IT controls in this fashion:

While the importance of IT controls is embedded in the COSO Framework, numerous observers have pointed out that it doesn’t do enough to help identify, document and evaluate those IT controls⁴.

For this reason, many companies have turned to COBIT because it focuses on IT governance using a framework of control objectives. ITGI defines corporate governance as a means of bringing IT decision-making into the same governance process that applies to other areas of the company’s operations, so that the company’s IT operations sustain and extend the company’s strategies and objectives⁵. The COBIT standard divides IT into thirty-four different processes under four major domains (plan and organize, acquire and implement, deliver and support, monitor and evaluate) and addresses five main focus areas (strategic alignment, value delivery, risk management, resource management and performance measurement).

⁴ “Information Security and Sarbanes-Oxley,” (February 17, 2004), available at <http://enterprisecurity.symantec.com>.

⁵ See “About IT Governance” at <http://www.itgi.org>.

COBIT may be a good starting point for companies that seek to comply with the internal control requirements of SOX. COBIT addresses the three elements of the term “internal controls” as defined by SEC Rules. Furthermore, many elements of COBIT apply to measures that would meet the COSO components that affect information technology, as illustrated below:

Affected COBIT Process or Domain:	COSO Component:	Control Environment:	Risk Assessment:	Control Activities:	Information & Communication:	Monitoring:
Planning and Organization	IT Planning	X	X		X	X
	Information architecture			X	X	
	IT organization & relationships	X			X	
	Communicate management aims/direction	X			X	X
	Management of HR	X			X	
	Compliance with external regs				X	X
	Assessment of risks		X			
	Manage quality	X			X	X
Acquisition & Implementation	Acquire/develop applications			X		
	Acquire technology infrastructure			X		
	Develop/maintain policies & procedures			X	X	
	Install/test applications & infrastructure			X		
	Manage change			X		X
Delivery & Support	Define/manage service levels	X		X		X
	Manage 3rd party services	X	X	X		X
	Manage performance & capacity			X		X
	Ensure system security			X	X	X
	Educate and train users	X			X	
	Manage configuration			X	X	
	Manage problems & incidents			X	X	X
	Manage data			X	X	
	Manage facilities		X			
	Manage operations			X	X	
Monitoring & Evaluation	Monitor change				X	X
	Adequacy of internal controls					X
	Independent assurance		X			X
	Internal audit					

The process of developing internal controls, however, is just the beginning of mending the holes in a company's SOX compliance. Once these controls are in place, SOX requires companies to engage in regular evaluation to ensure that these controls work.

Hoping the Patches Hold: Ongoing Evaluation of Internal Controls

SOX section 302 does not end with the requirement to implement internal controls. Sections 302(a)(4)(C) and (D) require the chief financial officer and chief executive to certify that they:

- (C) have evaluated the effectiveness of the [company's] internal controls as of a date within 90 days prior to the report [in which their certification appears];
- (D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date

Similarly, Section 404(a)(2) of SOX requires that each company annually assess "the effectiveness of the internal control structure and procedures... for financial reporting" for purpose of its annual "internal controls report."

Ongoing evaluation is not a new topic for information security. Testing and validation of security systems on a regular basis is a primary requirement to maintain reasonable network security. With respect to the information technology elements of the internal controls that companies adopt to comply with Section 302 (a)(4)(A) and (B) of SOX, this translates into documenting processes and systems, risk analysis and mitigation controls, and key control test strategies for the information technology systems that impact financial reporting.

Unlike typical information security testing processes, evaluation of the information technology elements of SOX internal controls must be done more than yearly and the results must be certified by the highest levels of management. In fact, according to 302(a)(4)(C), the evaluation process must be conducted at least quarterly, and the effectiveness of the controls must be certified in writing by the chief executive and chief financial officer under 302(a)(4)(C). Because of the certification requirements under 302, incomplete or slipshod evaluations can lead to significant sanctions for management.

As noted in the next section, each of these evaluation requirements feeds into the comprehensive disclosure requirements under SOX. Without effective evaluation of internal information technology controls, companies cannot adequately meet the disclosure requirements outlined below.

Showing Holes in Your SOX Compliance: Disclosure

Because many of the corporate scandals that fueled the passage of SOX were fed by corporate secrecy, the law contains a number of very thorough disclosure requirements. Unlike a diner at a Japanese restaurant who may be excused from removing his or her shoes because of embarrassing gaps in foot hosiery, embarrassment is not an excuse for failing to bare the holes in a company's SOX compliance.

As noted above, Section 302(a)(4)(D) of SOX requires companies to report how effective their internal controls have been on a quarterly and annual basis. Section 302(a)(5) of SOX contains two even more comprehensive disclosure requirements. This section requires the chief executive and principal financial officer to certify that they have disclosed to the company's auditors and the audit committee of the board of directors:

- (A) all significant deficiencies in the design or operation of internal controls... and any material weaknesses in internal controls; and
- (B) *any fraud, whether or not material*, that involves management or other employees who have a significant role in the issuer's internal controls (emphasis added)

In addition, SOX section 302(a)(6) requires the signing officers to indicate whether there have been significant changes in internal controls (or other factors that could significantly affect internal controls) after the date of last evaluation.

Taken together, these disclosure requirements under 302(a)(5) and (6) have some significant ramifications for information technology. The principals of the company cannot report deficiencies in design or operation of internal controls, or significant changes to them, unless they have the ability to detect and audit changes to the systems that support these internal controls. Furthermore, because the requirement of 302(a)(5)(B) extends to "*any fraud, whether or not material*" that involves management or others with the ability to influence internal controls, this heightens the need for use of network monitoring software and systems that will detect misuse by internal personnel and for policies and procedures that allow companies to monitor employees use of the company's information technology systems (and sanction them for misuse).

In addition to these requirements under 302(a)(5) and (6), Section 404 of SOX and the related SEC Regulations require companies to include a separate "internal controls report" with its annual report to the SEC. This report must "state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting," and as noted in the previous section of this paper, contain an assessment of the effectiveness of these measures.

Last but not least, Section 409 of SOX contains an ongoing requirement to quickly report unfolding events that may affect the company's financials or operations. Section 409 requires companies to disclose to the public "on a rapid and current basis" any information concerning material changes to financial conditions or operations of the company. From an information technology perspective, this may require companies to report a breach of security or a security vulnerability that might materially affect a company's financial conditions or operations. Although some commentators downplay the potential economic effects of a breach of security on a company, an incident in 2002 demonstrated how a trusted insider might use security to reduce the stock value of a company to his advantage. In this incident, a systems administrator for UBS Paine Webber inserted a logic bomb in the systems of 1000 Paine Webber officers shortly before he resigned, and then purchased a number of put options for the company's stock in the hope that the stock would fall when the logic bomb caused systems to crash, allowing him to profit. Paine Webber spent more than \$3 million to assess and repair the damage⁶.

The Stigma of Bad SOX Compliance: Responsibility, Penalties, Enforcement and Deadlines

The drafters of SOX sought to ensure that the law was much more than a toothless compliance mandate. To that end, the law contains significant penalties, an international scope and strict deadlines. The pattern of compliance prosecutions by the SEC prior to SOX demonstrates that the law will likely become the basis for a rising number of SEC prosecutions.

⁶ See "Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing 'Logic Bomb' on Company Computers," (December 17, 2002) (available at http://www.usdoj.gov/usao/nj/publicaffairs/NJ_Press/files/du1217_r.htm)

The question “who’s responsible?” is often the first one asked when a new law is passed. SOX places compliance responsibility squarely at the highest levels of the company. The internal controls, evaluation and disclosure requirements under 302, for example, are required to be certified in writing by no less than the principal executive officer and principal financial officer of the company. As noted in the penalties and enforcement discussions below, these are also the officers that face the stiffest penalties and to date have been the targets of most SEC prosecutions.

This responsibility does not stop at the U.S. borders. The law extends to overseas operations of companies publicly traded on U.S. exchanges. The internal controls required by SOX must be implemented worldwide for affected companies, which may prove tricky given cultural and legal differences overseas.

The tight deadlines for compliance also leave little room for error. The deadline for compliance with Section 302 was 30 days after the original passage of SOX, in 2002. The deadline for compliance with Section 404 depends upon the company’s market cap. Companies over \$75 million must comply as of their next annual report filed after November 15, 2004. Companies below this cutoff must comply as of their next annual report filed after July 15, 2004.

For companies and officers who fail in their compliance efforts, the penalties and fines are significant. Fines of up to \$1 million and prison time of up to ten years are the penalties for knowingly violating Section 302. If the violation is willful, the penalties increase to fines of up to \$5 million and prison time of up to 20 years. Furthermore, under Section 304 of SOX, if a company must restate its financial statements due to misconduct or material noncompliance with any financial reporting requirement, the principal executive and principal financial officer must *reimburse the company* for:

- (1) bonuses or other incentives or equity-based compensation during the 12-month period following issuance of the financial statements; and
- (2) profits from the sale of its securities during that 12-month period

Although SOX is a relatively new law, The SEC’s actions to date indicate that it will be vigorously enforced:

- In October of 2003, an Ernst and Young accountant was arrested for instructing other employees to destroy and backdate audit records concerning a bankrupt client⁷. The SEC charged that the accountant ordered another E&Y employee to alter change the date on his computer to make it appear that recently altered audit documents had been drafted during an original audit months earlier. The accountant was freed, on \$1million bail.
- In June of 2004, Symbol Technologies paid the SEC a \$37 million fine to settle securities law and SOX allegations⁸. The SEC alleged that the company and eleven of its executives violated federal securities laws (including the internal controls requirements of SOX) in efforts to inflate revenue and earnings figures. The actions against the eleven executives are still pending.

⁷ “Accountant Arrested Under Sarbanes-Oxley,” USA Today October 14, 2003.
http://www.usatoday.com/money/companies/regulation/2003-09-25-ernst_x.htm

⁸ “Symbol Technologies Agrees to Settle SEC Enforcement Action Charging the Company with Accounting Fraud,” June 30, 2004
(available at <http://www.sec.gov/news/press/2004-74.htm>).

- Former HealthSouth CEO Richard Scrushy is facing 85 counts that include charges of accounting fraud, use of ill-gotten gains and violations of the Sarbanes-Oxley Act for alleged accounting irregularities⁹. The government's allegations suggest that HealthSouth inflated earnings by \$2.5 billion. Scrushy faces up to 650 years in prison and \$36 million in fines.

As if these specific cases were not enough, a study conducted by the SEC indicates that the number of actions they have filed against companies for improper financial reporting has steadily increased¹⁰. The study indicates that over a five-year period from July of 1997 to June of 2002, the SEC filed over 500 such actions, and that the number has increased from 91 in 1997 to 149 in 2002. Of the 869 defendants named in these actions, the number of individuals prosecuted (704) far surpassed the number of companies (164). Most of these individuals were upper management. Given this trend, it seems unlikely to expect that the SEC will lessen the number of prosecutions now that it has SOX as an additional basis for violations.

On the other side of the "stick," of course, there is always a carrot. Some surveys have suggested that investors view compliance as a positive indicator of a company's value. **The Wall Street Journal** summed up the effect of compliance on investor confidence in this fashion:

Judging by public opinion, the law is a hit: A Harris poll sponsored by Movaris, a provider of Sarbanes-Oxley compliance software, earlier this year found 59% of investors believe the Sarbanes-Oxley Act will help safeguard their stock investments, and 57% say they would be very unlikely to invest in a company that didn't comply with the law. Supporters say investors are regaining their faith in markets, and view the Sarbanes-Oxley Act as a key factor in the process¹¹.

⁹ "Scrushy Indicted on 85 Counts," CFO (November 5, 2003) (available at <http://www.cfo.com/article.cfm/3010823?f=related>)

¹⁰ Securities and Exchange Commission, Report Pursuant to Section 704 of the Sarbanes-Oxley Act (available at <http://www.sec.gov/news/studies/sox704report.pdf>)

¹¹ "Is Sarbanes-Oxley Working?" The Wall Street Journal (June 21, 2004) (available at http://online.wsj.com/ad/article/ironmountain/SB108750495035740487.html?mod=sponsored_by_ironmountain).

Conclusion: Keeping up Your SOX Compliance

Companies faced with SOX clearly need to adopt a compliance process that addresses the control, evaluation and disclosure elements of Sections 302, 404 and 409. Because information technology is crucial to support and enable financial reporting and other company operations, information security technologies and measures must be adapted to meet these requirements.

Because the law and a company's operations will clearly change over time, companies that adopt a change auditing approach that includes strong IT governance measures are best positioned to equip the principal executive and principal financial officer (who have the ultimate responsibility for compliance) with the tools needed to fulfill their duties to implement and certify to the existence of internal financial controls and meet the evaluation and disclosure requirements of SOX. The General Counsel of GE was brief but straightforward when commenting on his view of SOX:

"Sarbanes-Oxley has nothing to do with culture. You either have it or you don't. If you don't have it, you'd better get it"¹².
—Ben Heineman, General Counsel, GE

One IT executive succinctly summed up his company's approach (and his department's role) in SOX compliance in this fashion:

"It's rare to have something literally fall from the sky that stops all of the projects that we had on the table from an IT perspective"¹³.
—Bobby Russell, IT Manager, First American CIG

If the prospect of having SOX fall from the sky disturbs affected companies, they can at least consider that it beats having a summons from the SEC fall from the sky. If that happens, of course, the company's executives may not end up dealing with SOX, but darning socks (prison issue), in an eight-by-five cell.

¹² "The Founding Father," Corporate Counsel (available at http://www.ge.com/en/commitment/governance/news&views/founding_father.htm)

¹³ "SOX Wars: CIOs Share Ideas, Fears on Sarbanes-Oxley Compliance," CIO News (available at http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci994763,00.html) (quoting Bobby Russell, IT Manager, First American CIG).



Audit Change. Prove Control.

www.tripwire.com

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA

www.tripwire.com/intl/uk

TRIPWIRE UK: +44 207 618 6512 FAX: +44 207 618 8001
78 Cannon Street London EC4N 6NQ UK