When SOX Meets Lean

Will they team up well or collide?

BY FRED GARBINSKI

The Sarbanes-Oxley Act of 2002 (SOX) is one of the most influential—and controversial—pieces of corporate legislation. Its original aim was modest. The methods of complying with it, however, were anything but. In this article I'll offer an overview of SOX and address:

◆ What are our experiences so far? How did we get to where we are?

◆ Where do we go from here? Is there any hope for sanity?

◆ Are there common denominators between SOX and Lean that will be the compass for the future? Or will SOX suck the life out of Lean?

Did anyone think that SOX would be as far-reaching or as controversial as it has been? I doubt it. I remember thinking when it was enacted that it was just a reemphasis of the Foreign Corrupt Practices Act (FCPA) and a typical, and quite frankly, not unexpected regulatory response to instances of corporate misconduct.

The government had been threatening to regulate auditing for years, claiming that self-regulation hadn't worked. Accountants had been looking over their shoulders for that same period, recognizing that as soon as another McKesson & Robbins, Equity Funding, or S&L crisis occurred, the government would make good on its threats and regulate auditing. Enron, WorldCom, Adelphia, Tyco, and others were just the last straw.

Q1: What are our experiences so far? How did we get to where we are?

Internal control is hardly a new concept. The definition has evolved over the years. In fact, the concept first appeared in the early 1900s with the need for accurate financial information and attestation to secure loans. Borrowers had to convince lenders of their capacity to repay, and financial information became the foundation on which those lending decisions were made. But lenders needed some assurances that those statements were prepared correctly, and, for that, they turned to groups of public accountants. These accountants realized early on that some reliance had to be placed on the underlying processes followed to prepare the statements, and from that need came the first definitions of internal control.

It wasn't until 1949, however, that an acceptable definition emerged. As Steven Root describes it, it was "one of several steps taken by an apologetic accounting profession in the aftermath of the scandal involving McKesson & Robbins. These steps were deemed necessary to prevent the fledgling Securities & Exchange Commission from exercising its statutory authority to set accounting and auditing rules for the private sector."

In 1977, the subject of internal control came of age as a result of the enactment of the Foreign Corrupt Practices Act. The FCPA made it illegal to maintain an inadequate system of internal control. What followed was a free-for-all of explanations covering how to recognize an adequate system of control.

The financial reporting fiascos in the late 1980s led the Treadway Commission to recommend that the various concepts and definitions of internal control be integrated. The result was the publication by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) of its internal control framework document (*Internal Control—Integrated Framework*) in 1992. (For more information about the above section, read Chapter 3 in Steven J. Root's *Beyond COSO: Internal Control to Enhance Corporate Governance.*)

Important Points from an Historical Perspective

The important points to keep in mind from this historical perspective are:

◆ The public accounting profession managed the thinking on internal control for most of the 20th Century, and those definitions were influenced by the questions raised concerning the extent to which auditing work was necessary.

◆ The work of COSO was strongly influenced by the perspectives of the public accountant even though other interested parties participated in developing this framework.

◆ Recognition was growing that internal control over financial reporting—while remaining very prominent—is but one aspect of internal control. COSO, for example, agreed on three categories that need to be effective: effectiveness of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

The scandals of 2001 and 2002 (Enron, WorldCom, Adelphia, et al.) tipped the scales. Congress had to do something. Enacting SOX, some argue, will become known as the perfect financial storm, citing that all three elements existed: the heat from the rising stock market that swept the nation throughout the 1990s, the cold from the economic downturn that blew in at the end of the decade, and, before the storm could blow out, a new hurricane that rose in the form of accounting irregularities and other questionable practices. The combination of these forces caused the Bush administration, Congress, and regulators to act swiftly and categorically. Although the aftermath of this storm may linger for years, its immediate effects have already been felt. (For more information on the "perfect storm" concept, see the article by Frederick R. Bellamy and W. Thomas Conner, "Sarbanes-Oxley Act of 2002: The Perfect Storm," in the November/December 2002 issue of *NAVA Outlook*.)

Major Provisions

Some of those effects have come about by virtue of the provisions of the law. Others, that many are finding to be more ominous, are due to how the requirements are being implemented. Essentially, the government is again attempting to prevent individuals from wrongdoing by passing more stringent legislation. This approach brings to mind Einstein's definition of insanity: "doing the same thing over and over again and expecting different results." Nonetheless, SOX requires:

◆ ***Audit committees*** that consist solely of independent directors, at least one who is designated as a financial expert.

◆ ***Auditing standards*** that are set by the Public Company Accounting Oversight Board (PCAOB). Auditing firms are required to register with and be monitored by the PCAOB.

◆ ***Auditors*** are required to issue two additional opinions. One of those covers management's process of establishing and evaluating its controls. The second is the auditor's opinion on the effectiveness of those controls.

◆ ***CEOs and CFOs*** are required to

—Certify that it is their responsibility to establish and maintain adequate internal control over financial reporting;

—Identify the framework used to evaluate the effectiveness of internal control over financial reporting;

—Conduct an assessment of the effectiveness of the company's internal control over financial reporting as of the year-end; and

—State that their company's auditor has issued an attestation report on management's assessment.

It's clear that COSO failed to alter the fixation on financial reporting controls and the importance placed on such controls in deterring financial reporting fraud. Perhaps it's true that you tend to drift to the familiar, especially in times of crisis. This is no different. This fixation on financial controls overrode any of the other considerations when SOX was being implemented, so the financial reporting controls took center stage, and only those elements of COSO were considered. The auditors held all the trump cards. Accordingly, management, driven by the need to satisfy the auditors' requirements, fell into the first-year trap of near blind obedience.

Q2: Where do we go from here? Is there any hope for sanity?

Let's turn to our second question: Where do we go from here, and is there any hope for sanity? I think so. In April 2005 and again in May 2006, the SEC held a roundtable in Washington, D.C. It was a "who's who" list of panelists (top executives or board members from the NYSE, NASDAQ, CalPERS, Government Accountability Office (GAO), the Big 4 public accounting firms, and some of the biggest names in corporate America, including General Electric, Microsoft, Dow Chemical, Lockheed Martin, Eli Lilly, and Aetna) as well as all SEC commissioners and PCAOB board members. More than 60 participants were involved in separate panel discussions, and, although they were a diverse group, the themes were consistent throughout the day: "It is not the legislation that needs to be fixed but, rather, the implementation of 404 through the auditors, PCAOB, and SEC that needs to be addressed." The most popular topic was the need to control the substantial and unanticipated costs of Section 404 compliance.

SEC and PCAOB Issue New Interpretations

After the April 2005 roundtable, the SEC and the PCAOB issued interpretations to address the issues raised there. In its statement, the SEC said:

"An overarching principle of this guidance is the responsibility of management to determine the form and level of controls appropriate for each company and to scope their assessment and the testing accordingly. Registered public accounting firms should recognize that there is a zone of reasonable conduct by companies that should be recognized as acceptable in the implementation of Section 404." (You can find this at www.sec.gov/news/press/2005-74.htm.)

Shortly after this guidance was issued, in a June 15, 2005, speech titled "SEC in Transition: What We've Done and What's Ahead," then SEC Commissioner and Acting Chair Cynthia A. Glassman noted some of the strengths and failures of SOX Section 404. "There is no question in my mind that the implementation [of SOX Section 404] has been misdirected," Glassman said. "What was meant to be a top-down, risk-focused management exercise became a bottom-up, 'check the box,' auditor-driven exercise."

From these interpretations, it's clear that the SEC and the PCAOB heard the message and acknowledged that an auditor-led process wasn't the intent of this legislation and are taking the steps to move these requirements in the right direction. Has the message been heard? If you consider that immediately after this guidance was issued, accounting firms stopped pressing sample size and key controls issues and began to listen to other control mechanisms that are equally effective, I would say "yes." Up until these interpretations, guidance to the accounting firms' clients and staff was that the approaches needed to be essentially the same as what the firm had prescribed. But after the 2006 roundtable, it was clear that not much has been done and that additional guidance on what management needs to do is desperately needed.

The Case for Moving Beyond Compliance Is Compelling

So, what should we do now? We had 60 emissaries go to Washington twice and argue the case. They came away with the SEC and the PCAOB acknowledging that SOX implementation is costing too much and that auditors might have been and still are overconservative in their interpretations. The SEC acknowledged that management should take the lead. After all, as one panelist pointed out, we have been designing, monitoring, and improving these processes longer than many of the auditors have been alive.

Remember, unless we can make this happen, it isn't going to matter. We can adopt it with enthusiasm and get caught up in the intellectual excitement, but if we don't have the interest in the how's, it won't be implemented.

Former SEC Chairman William Donaldson sees it as a three-step process: comply, sustain, and improve. Comply because there is a legal obligation to do so. That thought can become the lever needed to move us from the status quo. He then calls for companies to sustain it by enlisting other functions in the initiative. It's apparent to many

Figure 1: QSI/Lean Office/SOX Integration and Project Plan

PROCUREMENT

PROCUREMENT PROCESSES
- Supplier Selection
- Analysis
- 1 Purchasing Product
- Determine Inventory Levels
- Production Needs
- Expense Purchases
- P-Card Use

INBOUND PROCESSES
- Receiving
- Inspection
- Move to Stock
- Rejected from Inspection
- 3 Goods Not Received in System
- Communicated Goods Ordered to Receiving
- Goods Delivered to Dock
- Goods Unloaded

ACCOUNTS PAYABLE
- System Access
- PO and Non-PO Invoices
- 2 Autovouchering
- Debit Memos
- Month-End Close

DISTRIBUTION

CUSTOMER SERVICE
- Quoting
- Order Taking
- Pricing

NEW PRODUCT LAUNCH
(Lean Office, not SOX Process)

OUTBOUND
- Pricing
- Order Changes
- Shipping
- Invoicing
- Producing the Order
- Credit Checks
- Shipping

ACCOUNTS RECEIVABLE
- Return Process (R&A, Credits)
- Collection
- New Customers

PROCESS FUNDS
- Cash Application
- Cash Receipts

CONVERSION

PAYROLL & BENEFITS
- New Employees
- Process Payrolls
- Hiring and Terminations

PROCESS FIXED ASSETS
- Purchase of Asset
- Capitalization
- Completion
- Process AFE

TOOL ROOM
(Lean Office, not SOX Process)

TOOL DESIGN
(Lean Office, not SOX Process)

SUPPORT

ACCOUNTING
- Analyze and Reconcile
- Financial and Management Reporting
- Product Costs
- Reserves and Allowances

MANAGE IT

COSO processes used as the framework for SOX are integrated into the Lean processes.

that you can't sustain it as a finance-only work product. It will become a one-off project conducted once a year, driven by finance, with a clean year-end SOX opinion as its only goal. The only measure of success will be no material weaknesses. No one will explore opportunities to improve internal controls, to improve performance, or to improve reporting. Like other similar initiatives, it will languish on the laptops in the "Oh, my God, do I really have to do that again?!" folder. What's worse is that we will be left with auditor-designed processes that will be laden with all the documentation, sign-offs, approvals, and controls that will strangle any attempt to implement Lean systems.

On the other hand, we management accountants can view it as an opportunity to reclaim this responsibility from the auditors. Yes, reclaim it. The auditors assumed they had the authority through the auditing standards, but those standards setters gave the baton back to management in each of their post-roundtable interpretations. A friend of mine at another company stated in a moment of sheer frustration with his accounting firm: "Damn it, this is our company, and these are our processes. We have designed them to be effective, efficient, and provide the necessary control. I'm not going to change them just to satisfy an auditor when I know it's nonsense."

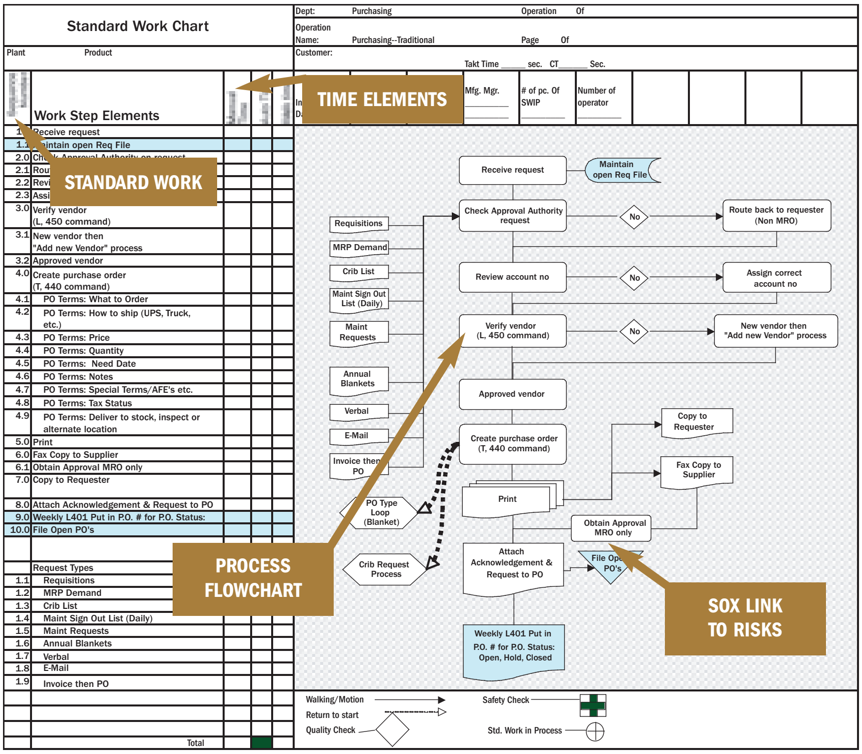
Q3: Are there common denominators between SOX and Lean that will be the compass for the future? Or will SOX suck the life out of Lean?

Where do we begin?

It's ironic, but SOX and Lean actually have a lot in common. For example, both are process oriented; both are concerned with control; both are concerned with managing risk; both believe the processes need to be documented, evaluated, and improved; both believe culture is important; and both value integrity and respect for people.

The differences are the lenses through which each is viewed. In SOX (up to now), the public accountant's view has prevailed. It's understandable since all through history, from the early definitions through SOX, public accountants have taken an active role in defining internal accounting control since they had the most at stake. In Lean, it's senior-management led. The definitions, direction, and philosophies aren't at all consistent from one firm to another since the concepts are just beginning to

Figure 2: Standard Work Chart



product. Since COSO is process oriented as well, it's easy to fit the COSO elements into each. This also becomes helpful in identifying the process owners. For example, purchasing managers can easily fit as the procurement process owners, the manufacturing or operations managers as the conversion process owners, and sales or marketing managers as the distribution owners. The objective is to use your organizational structure and fit the elements of COSO under that structure. It visually identifies who is responsible for each COSO element. In this way, as Lean kaizen events are conducted (shown as numbered kaizen bursts in Figure 1), these COSO elements will be subject to review, evaluation, and improvement during that event. Likewise, the associated COSO risks will also be explicitly addressed as shown later.

be understood and take root.

Unlike COSO, there is no group of organizations that have come together to define Lean. Almost everything that's available is case-study driven, and most of those deal with designing or manufacturing a product. The Institute of Management Accountants (IMA®), however, recently published two Statements on Management Accounting (SMAs) about Lean. One is *Lean Enterprise Fundamentals*, and the other is *Accounting for the Lean Enterprise: Major Changes to the Accounting Paradigm*. A third SMA, *Applying Lean Fundamentals Beyond the Manufacturing Floor*, is forthcoming. (You can find these at www.imanet.org/smas.)

Notwithstanding the dearth of guidance, I have made an attempt to integrate the major elements of Lean with COSO's Integrated Framework. Although this approach is still in its formative stages, here are the steps followed in several divisions of a *Fortune* 100 company.

Step 1: Integrating the COSO Elements into Lean Categories

The first step is to take the elements contained in the COSO framework and regroup them into organizational categories. As shown in Figure 1, those categories are procurement, conversion, distribution, and support. They were chosen because they generally follow the flow of

Step 2: Conducting Kaizen Events and Integrating the COSO Elements

Step 2 is done during a kaizen event. Almost all events begin by doing a process map to identify the work steps, the flow of the work, and the time taken (cycle time and the like). As you can see in Figure 2, all the work elements are shown along with a process map and time elements. What's unique in this map is the color coding of activities that relate to SOX risks. Color coding makes those activities visual for the entire team. That signal means that this activity is the responsibility of the financial expert on the team. Similar to the expert in the "stop and fix" Lean environments, each team has a financial representative whose role is be the "custodian" of those activities addressing a SOX risk. To help them show that integration even more clearly, Figure 3, which is prepared and maintained by the financial expert, shows each risk contained in the COSO Integrated Framework with the cross-references to the work steps contained in Figure 2. Another feature (that isn't shown) is a cross-reference to the testing or monitoring activities that are performed within the process. In this way, all the SOX requirements (documentation, risk identification, and testing) are part of each Lean event, thereby subjecting it to review and improvement, and that specific improvement is under the guidance of a financial expert.

Figure 3: SOX Risks—Integration with Lean

	COSO RISKS	COSO	COSO REF	IAD REF	CONTROL ACTIVITIES (Links to Standard Work)
1	Out-of-Date or incomplete price information —pay appropriate Price	O	page 80	page 23	Monthly PO audit>$1,000 (PM) >$10,000 (Acctg) Spending controls AP reviews price lists & PO price match User Access Control Network Procurement Phases 1 and 2
2	Purchase orders may be lost —record authorized POs completely and accurately	OF	page 82	page 24	AP & Receiving compare against PO file
3	Inadequate policies and procedures to prevent unauthorized use.	OF	page 82	page 24	Yearly review of user access Access Limited to authorized personnel P-Card issuance is approved by Dept. Manager/controller P-Card use is controlled by corporate policy
4	Inadequate vendor screening, including periodic re-qualification of existing vendors —identify and purchase from vendors capable of meeting the entity's needs	O	page 78	page 21	Network Procurement Phase 1 & 2 Supplier performance report reviewed quarterly New inventory suppliers complete self-evaluation form Majority of production suppliers are third-party certified
5	Unavailable or inaccurate info on inventory levels or production needs —order appropriate quantity at appropriate time	O	page 81	page 23	DSI Kanbans OTD for supplier MRP Report
6	Purchase orders are not entered into the system on a timely basis	O	page 81	page 24	PO Requisitions in Queue—visual perf measures standard work
7	Unavailable or inaccurate info on items ordered but not received	O	page 81	page 24	Past-due report reviewed weekly for production items Daily task includes maintaining open POs
	OTHER RISKS NOT INCLUDED				
	Unavailable or inaccurate information about fraudulent acts or other improper activities or vendors		page 79		
	Poor communication of operations' or other activities' needs		page 79		
	Inappropriate production specifications		page 79		

Step 3: Entity-Level Processes that Make Material Weaknesses Unlikely

The final step in the integration with Lean is articulating how a Lean environment—with its structure, accountability, and monitoring—reduces the risk of a material weakness in financial reporting. The arguments that have resonated well with outside auditors and other practitioners are:

Small units. Create small organizational units. When they are small, financial errors become obvious. Consider the size of a typical value stream where some experts suggest they be limited to 25-125 people. When financial results are reported for units of that size and are monitored frequently, even small reporting errors have a greater likelihood of being noticed and acted on. It's no different from highly decentralized environments. Where operating divisions are all less than 5% of sales, the likelihood of material errors, whether they are intentional or unintentional, becomes less as the units become smaller.

Accountability. Only give them what they need to control. Separate the categories of assets, liabilities, and related operating results into that which they need to and can control. What they need are all the things necessary to service the customer, including designing product, taking orders, procuring materials, producing the product, and finally shipping and billing the product. From a financial statement standpoint, that means they need billing and receivables, purchasing and payables, fixed assets and payrolls. From a systems standpoint, they need simple approaches that are governed by standard work and IT systems to support them. All the other accounting stuff is muda (a Lean term that means waste) that creates com-

CROSS REFERENCES	REFERENCE	
Std Work Mtls Mgr (>$1,000) and Acctg (>$10,000)	step 1.1	step 1.1
Std Work All Managers	step 1.2	
Std Work Acctg	step 1.2	
Std Work IT; Acctg	step 1.1	step 1.3
Std Work Mtls Manager	step 1.3	
Std Work Acctg and Receiving Std work	step 1.4	step 1.1
Std Work Team (IT and Acctg)	step 1.1	step 1.3
Std Work IT	step 1.2	
Std Work Acctg	step 1.5	
Std Work Acctg	step 1.5	
Std Work Mtls Mgr for all items in this category	step 1.3	
	step 1.4	
	step 1.5	
	step 1.6	
Std Work and Performance Measure Mtl Mgr	step 1.7	
Std Work Mtls Mgr to oversee and develop Kanban Stds. Others implement	step 1.8	
Performance Measure that is tracked by Purchasing	step 1.9	
Std Work Mtls Mgr	step 10.0	
Standard Work Purchasing	step 1.1	
Std Work Mtls Manager	step 1.11	
Std Work Purchasing	step 9 and 10	

plexity and variety and increases the risks. Move those into shared services centers that specialize in those particular areas, for example, treasury and tax matters.

Monitor. Review the results weekly, monthly, quarterly, and annually. This is the hallmark of a Lean environment where the work is monitored continuously and immediate action is taken when a problem is noted. This is no different. Financial information, along with operating information, should be monitored frequently and acted on to determine underlying causes and necessary corrective actions.

What's Needed to Integrate Lean with SOX?

It goes without saying that active participation—not cheerleading from the sidelines—is essential. Beyond that you need to:

- ***Understand*** the internal control program and the financial reporting process.
- ***Map*** the systems that support internal control and the financial reporting process.
- ***Identify*** risks related to the systems.
- ***Design and implement*** controls designed to mitigate the identified risks.
- ***Document*** controls.
- Ensure that controls are ***updated and changed***, as necessary, to correspond with the processes currently in effect.
- ***Develop key performance indicators (KPIs), and monitor*** controls for effective operation over time.

The choices are simple. Either you accept the challenge to incorporate SOX into your Lean initiative or you don't. If you choose to integrate, each process can be reviewed once and contain the requirements of each initiative. If you choose not to integrate, processes will need to be examined as many times as there are initiatives. The many-to-one approach is simply not an efficient way of approaching process reviews. Each initiative then requires a separate review, and the scope of each must be designed to meet separate objectives. This is hardly a way of incorporating any initiative into an organization's DNA. Alternatively, in the one-to-many approach, each process review would be designed to contain all the requirements, and each initiative (Lean, SOX, total quality management (TQM), et al.) would be designed to meet all the objectives. This is clearly a more effective way of addressing process requirements and can easily be sustained by becoming part of the organization's DNA. It's your choice. ■

Fred Garbinski recently retired with more than 35 years of Lean Accounting and financial reporting service with a Fortune *100 company and, before that, with Deloitte. During that time he led a number of financial initiatives including Reengineering Finance, Lean Accounting, and, most recently, Sarbanes-Oxley. You can contact Fred at (216) 702-1672 or fgarbinski@adelphia.net.*

Note: This article is an excerpt of a chapter in the soon-to-be-released book *Lean Accounting and Performance Measurement: the Relentless Pursuit of Perfection* by John Wiley & Sons, Inc. For permission to use the article in any way, please contact the author.