

# On Optimizing SOX Compliance

*Leading Retailer Shows the Way*



This publication contains general information only and Deloitte & Touche LLP is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte & Touche LLP, its affiliates and related entities shall not be responsible.

# On Optimizing SOX Compliance

## *Leading Retailer Shows the Way*

Corporate finance departments and C-suite executives got some long-awaited clarity with the recent approval and issuance by the Securities & Exchange Commission (SEC) of new guidance around Sarbanes-Oxley (SOX) Section 404 reporting. By encouraging companies to incorporate risk considerations in their 404 compliance work, the guidance provides business executives greater flexibility over controls assessment efforts and paves the way for SOX 404 compliance processes to produce benefits that are likely to outweigh, or at least counter-balance, any perceived compliance burdens.

Working in collaboration with the SEC, the Public Company Accounting Oversight Board (PCAOB) underscored support of non-prescriptive, principles-based requirements when it subsequently approved revised guidance for auditors that aligns with the SEC's risk-based approach. The new guidance is expected to go a long way toward improving the processes required to comply with Section 404—for both companies and auditors.

### Aligning the “spirit” and the “letter” of the law

This new stage of 404 compliance presents an unusual—and distinct—opportunity to optimize a company's overall SOX implementation efforts. After all, the “spirit” of SOX is grounded in strong ethics, good governance, and reliable financial reporting. Now, the SEC and PCAOB have interpreted the “letter” of the law in a manner that may well help many companies achieve compliance at a reduced level of management effort.<sup>1</sup> By emphasizing a risk-based approach that effectively leverages a company's entity-level internal controls and IT tools, opportunity-oriented organizations can improve their ability to prevent material errors, deliver enhanced business support functionality, and enhance the overall risk intelligence of the organization. In short, they can turn SOX compliance into greater business efficiency and effectiveness.<sup>2</sup>

Some far-sighted financial executives saw the potential advantages of a risk-based approach well in advance of the recent guidance. Such was the case with Jim Brigham, vice president of Internal Audit Ethics and Compliance and

Asset Protection for PETCO Animal Supplies, Inc., a \$2.5 billion retailer headquartered in San Diego, CA, and a SOX optimization client of Deloitte.<sup>3</sup>

PETCO was founded in 1965 and operated for most of its history as a public company, until July 2006, when it was acquired by two private equity groups. As a public company, says Jim Brigham, PETCO began adopting SOX 404 compliance standards in 2004, earlier than many other companies. When he joined in January 2006, company management had targeted the SOX 404 compliance program for improvement, and Jim immediately was able to identify opportunities for streamlining existing efforts. Mainly, he recognized that the company had been erring on the side of being overly cautious, thereby driving up compliance costs with many unnecessary steps. Jim brought in a team of Deloitte SOX compliance professionals to assist, based on their experience in implementing principles-based approaches to SOX work.

### Rationalized controls process led the way

After implementing a rationalized controls process, Jim and the internal audit team were able to reduce the total number of controls, improve testing, reduce project cost, and better organize the SOX project under a top-down, risk-based approach. Despite the fact that the company is now private and no longer required to abide by SOX standards, the realized benefits of having done so has driven continuation of the SOX program Jim and his team put in place.

<sup>1</sup> Organizations should note that a reduction of management activity around Section 404 compliance may have unintended consequences. The PCAOB's new audit standard might result in less auditor effort, or repositioning of existing effort towards areas of higher risk and away from areas of lower risk. But if management reduces its effort substantially (which it could under the SEC's guidance), this might well result in MORE audit effort. Some observers refer to this potential scenario as “the seesaw effect.”

<sup>2</sup> For more Sarbanes-Oxley-related guidance, visit [www.deloitte.com/us/sarbanes](http://www.deloitte.com/us/sarbanes).

<sup>3</sup> Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names “Deloitte,” “Deloitte & Touche,” “Deloitte Touche Tohmatsu,” or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein. Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu. In the United States, services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP, and their subsidiaries), and not by Deloitte & Touche USA LLP.

## Closer Look at A Top-Down, Risk-Based Approach

The new guidance allows management to identify the risks they believe pose the greatest threats to soundness of financial reporting without necessarily testing a long list of processes and controls that may or may not represent potential problems. In other words, good business judgment is a major factor. A few key questions help drive effective enterprise-wide decision making, including:

- Is the area to be tested critical to the proper operation of key controls that prevent or detect material misstatements?
- Have certain major risk factors been taken into account, such as volatility, subjectivity, and fraud?
- If a process or control risk exists, how might it be mitigated?

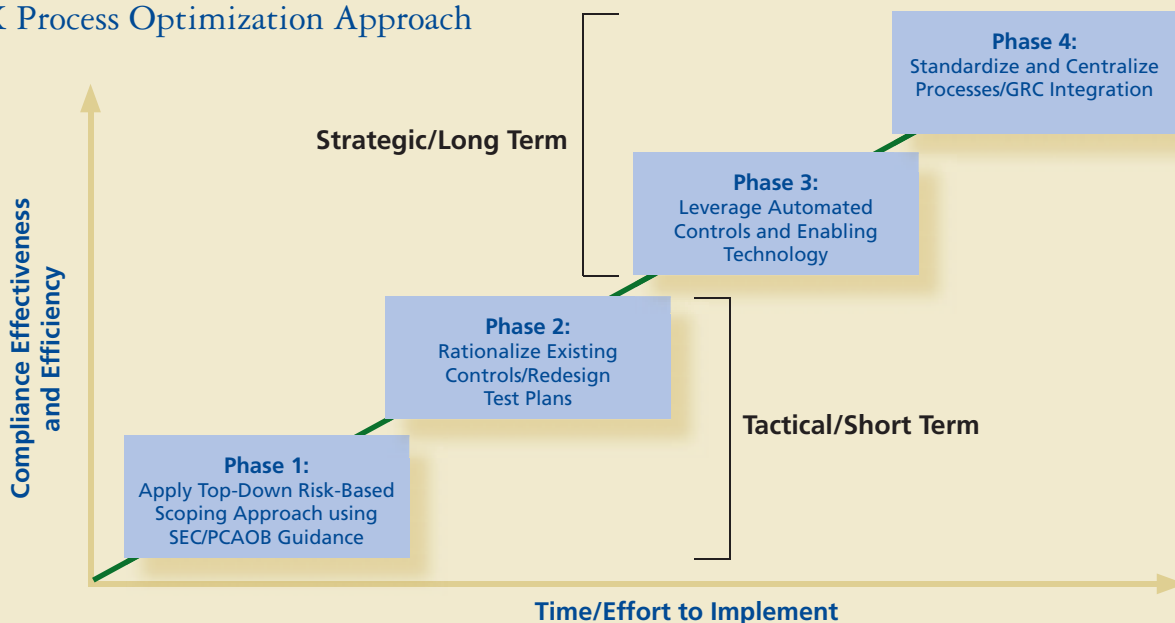
In highlighting the key dynamics of his project, Jim says the effort “probably has paid for itself 10 times over in reduced costs. Moreover, it allows us to get our internal auditors back to more internal, operational auditing. In summary, I firmly believe that we are maintaining a strong system of internal control at less cost and with less effort.”

## Case study points to best practices

According to Beth Kaplan, a director in the Audit & Enterprise Risk Services practice of Deloitte & Touche LLP, the PETCO story underscores some leading practices associated with implementing a SOX 404 optimization program, including the importance of leveraging company-level controls; the value of automated controls (making the process more reliable and easier to test); emphasis on self-assessment as a valued technique for management to evaluate the effectiveness of internal control over financial reporting; and leveraging continuous controls monitoring to conduct 100 percent testing versus sampling, where it is smart to do so.

At a recent Dbriefs for Financial Executives webcast, Beth interviewed Jim Brigham of PETCO for his perspective on his company's experience in implementing its SOX compliance program.<sup>4</sup>

## SOX Process Optimization Approach



Professionals from the Deloitte U.S. Entities view effective SOX implementation as a four-phased approach for getting the control environment integrated into the typical people, processes, and technology practices of the company. These phases are frequently referenced in the PETCO case study, so following is a guide to the four steps:

**Phase 1:** Applying a top-down, risk-based approach.

**Phase 2:** Rationalizing the existing control design; looking at a risk-based test plan.

**Phase 3:** Leveraging automated controls and enabling technology; getting closer to a continuous control environment and monitoring practices.

**Phase 4:** Standardizing and centralizing processes; adopting integration of governance, risk, and compliance processes throughout the organization.

<sup>4</sup>Deloitte's Dbriefs for Financial Executives webcast, "The Next Stage of Section 404: Opportunities for Management to Optimize Efforts," held on April 26, 2007. See the inside back cover for information on viewing the Dbriefs.

The following discussion provides a useful and exemplary case of how one executive leveraged Sarbanes-Oxley to achieve real benefits—including cost savings—for his company:

**Beth:** Jim, PETCO was an early adopter of SOX optimization. Give us some background on the series of steps that led to the current state of these efforts.

**Jim:** Back in 2004, the company took an approach that started with an overall scoping document and then worked from the bottom up, using Microsoft Word and Excel spreadsheets for control matrices. Company-level controls and system controls weren't really woven into the project nor relied upon. In 2005, there was almost a repeat effort of the 2004 compliance project with some additional minor recognition of IT controls, but significant dollars were being spent for outside assistance to complete the project. When I joined in January 2006, senior management wanted change and I saw opportunities to streamline the SOX effort, including reducing internal audit involvement and outside consultant spend; reducing the number of key controls; improving the testing approach; and approaching the process with a top-down, risk-based approach. Fortunately, all of this resulted in reduction of project costs and better organization of SOX implementation.

**Beth:** Phase 1 involves looking at risk factors such as volatility, subjectivity, fraud, lack of GAAP knowledge, previous significant errors, IT dependence, and absence of a monitoring function, among others. How have you made this work in your organization?

**Jim:** The very first component I worked on with the audit committee and senior management was an enterprise-wide risk assessment. The results of that assessment helped define our SOX project, including validating some key risk areas and downgrading others. We did about 50 candid interviews with senior management, and they were forthcoming about where they felt the risks were. That also was a good learning experience for me being new to the company. On the flip side, I think the process helped strengthen management's awareness of risk and their support for our go-forward program. The new SOX approach effectively brought together management perspectives with the risks identified through the holistic assessment process.

**Beth:** One of the main topics addressed by the new guidance relates to company-level controls. Can these really help minimize some of the transaction-level testing and monitoring that you do?

**Jim:** PETCO has done a good job of identifying key process controls. Now, our new approach has further enhanced that effort by also identifying what company-level controls could mitigate identified risks. Take payroll, for example: We were able to take key controls from 20 down to eight and then we went further by prioritizing those key controls into areas of high, medium, and low risks.

We used a graphical tool that helped us matrix and vividly portray process- and company-level controls and demonstrate

clearly our progress. This approach made it easy to see where we had duplication in covering risks, and at the same time it was easy for management and our external auditors to "visualize" our logic. Ultimately, we were able to reduce our key financial controls from more than 300 down to about 190, or about a 40 percent reduction; and we brought our key IT controls down from 190 to 23, or almost a 90 percent reduction. So, the tool was very helpful in getting us to those important points.

#### Improved Risk Mitigation with Fewer Controls

Type of key controls	Results in Numbers	% Reduction
Financial	307 to 190	38%
IT	190 to 23	88%

**Beth:** Can you describe a few critical success factors?

**Jim:** First of all, internal audit initially owned SOX compliance at PETCO. While we worked with management, we took responsibility for really driving the project and for the testing and the documentation. Second, early on, we recognized that one key success factor would be using a rationalization approach that provided an efficient means for keeping senior management and the audit committee informed. In fact, when we did the RFP for a provider to work with us on this process, we looked for a firm who could enable the whole thought process—why this control or not this one, support that decision, and help make it easy for senior management and the audit committee to understand what we were doing. That's where the tool described previously came in so handy.

We are in Phase 3 now, having gone through the rationalization part of the project, but we will continue to go back each year to Phase 2 and Phase 3, because we want to make sure that we account for changes in controls and updates in systems and other considerations that need to be taken annually.

**Beth:** Was there any initial concern that management, your CFO, or your auditors had about venturing into this rationalization effort and, if so, how did you mitigate some of those concerns?

**Jim:** Our CFO was interested in taking aggressive action in this area. I think he also felt that we were doing more [SOX compliance work] than was necessary in the past and so he was very supportive of this effort to arrive at an organized, streamlined approach to SOX. Our outside auditors also were supportive of it and I think they actually ended up rationalizing some of their approaches as well.

**Beth:** How did all of this change affect staffing in your internal audit department?

**Jim:** We have 11 professionals in our internal audit department, and initially I would estimate nine of the 11 were all supporting SOX. After we went through this process, we came down to two people who now support SOX—and we haven't yet pushed the testing out to control owners in the business units.

We also experienced significant reduction in outside consulting dollars—by hundreds of thousands. In addition, we achieved other efficiencies. In the 2006 audit, for instance, our external auditors were able to rely on our SOX documentation more than ever before. We're not in any hurry right now to push testing out to the control owners, but eventually that is where it will end up and then internal audit will become more of a quality assurance part of the process.

Nevertheless, the increased awareness in our company of internal controls and the need for those controls to be effective has really made SOX part of our business, which is one reason we aim to remain SOX compliant even though it isn't required of a private company. Our investors are very keen on having us remain well controlled and they see the SOX project and that whole program as key to maintaining that status.

**Beth:** So you are now in Phase 3, which gets into the concept of continuous control monitoring. We are seeing a great deal more continuous monitoring in certain organizations, because a 100% sample is certainly better than small sample sizes, especially when you're looking for fraud or anomalies within transaction data. You've mentioned that as a retailer, you certainly have that interest. Can you describe your experience in this area?

**Jim:** As a transaction-heavy retailer, we have a tool called XPR that actually filters every transaction at every register in the company every day and kicks out transactions that look abnormal. For example, one of the problems encountered in retail is fraudulent refunds and another is fraudulently voided transactions. We are able to use a tool that monitors and identifies activity that resembles these problems and we jump on top of the issue immediately.

Use of the XPR tool has reduced a lot of sales audit testing. You still look at the process-level controls such as the daily balancing and flowing from the sales information into the cash deposits and those types of topside reconciliations, but the detailed testing that we would look at in transactions has all been eliminated because of the XPR tool.

**Beth:** What have been the key benefits to PETCO of putting forth this whole program?

**Jim:** Well, I think the key benefits have been, first of all, significantly reduced cost of compliance, both internally and for outside consulting costs. A lot of that savings is a result of the control rationalization approach. In addition, we now have a staff that is more aware of risk-based auditing, and we have a better organization of our SOX project. You know, I believe overall what we are doing is a better job and we are doing it for a lot less cost.

**Beth:** Well, that is great preparation for the final phase of the process, which is when we see enterprise risk assessment baked into the overall governance and compliance processes of the organization. In other words, it is no longer a "carve out" or a separate piece of the business. It is where we expect to start hearing management use terms like "risk intelligence," implying a better understanding of where risks are and how

they're being monitored and/or mitigated. Jim, we appreciate you sharing your experience and perspective of bringing to life a 404 implementation program and controls rationalization approach at PETCO. Any concluding words of advice?

**Jim:** Yes, there are three key points for other finance executives to remember in the execution of a program. First, you must have senior management behind it. They have to believe in the process and, in particular, the CFO has to support it. Second, it helps to have a professional team with you on this journey; professionals who are objective and understand the relationship between internal audit, management, and the outside auditors, and who bring excellent qualifications and credentials to the table. And third, you should keep your external auditors apprised of your activities, so they can assess the impact of planned actions on the audit.

## Beth Kaplan's Key Takeaways

Under the new guidance, management and auditors will be able to spend much more quality time addressing their most meaningful control and reporting issues on a proactive basis. At the same time, companies can also position their organization through better risk identification and mitigation to avoid the cost and reputation damage of material restatements. SOX optimization potentially can generate significant savings and performance improvements, particularly when it is viewed and treated as a continuous improvement process. And, as savings and improvements are established and acknowledged, making the case for more fundamental changes in operations, such as automation and continuous controls monitoring, will likely become easier to justify and implement.

Use of the new SOX optimization methodology has the potential to play a major role in process improvement, enhanced alignment of technology with business goals, and integrated compliance processes. Executives who spearhead a SOX optimization project can help drive their organizations toward greater value generation and sustainability.

---

## Bios

*Beth Kaplan, director in the Audit & Enterprise Risk Services practice at Deloitte & Touche LLP, serves global clients in executing their internal audit plans and has overseen SOX 404 readiness and testing engagements at a number of major companies. Previously, she worked for 25 years in various corporate audit, finance, and operations roles, including controller and CFO. She used this experience in her role as a member of the Deloitte team that developed their proprietary SOX 404 optimization methodology and tools to assist clients in implementing effective and efficient internal controls procedures.*

*Jim Brigham is the vice president of Internal Audit Ethics and Compliance and Asset Protection for PETCO Animal Supplies, Inc. PETCO is a \$2.5 billion retailer headquartered in San Diego. Prior to PETCO, Jim was a senior manager with Deloitte & Touche LLP's Enterprise Risk Services practice in Dallas. He is an internal audit and retail specialist with more than 25 years of experience with national and regional retailers.*

## Dbriefs for Financial Executives

We invite you to visit [www.deloitte.com/us/dbriefs](http://www.deloitte.com/us/dbriefs) to join the Deloitte Dbriefs webcast series. The Financial Executives series helps you stay on top of all the latest issues and strategies in:

- Corporate Governance
- Driving Enterprise Value
- Financial Reporting
- Private Companies
- Sarbanes-Oxley
- Transactions & Business Events

## Contacts

### **Tom Connors**

Partner, Audit & Enterprise Risk Services  
National Leader of SOX Consulting Services,  
Audit & Enterprise Risk Services  
Deloitte & Touche LLP  
+1.212.436.2617  
[tconnors@deloitte.com](mailto:tconnors@deloitte.com)

### **Stephen Wagner**

Managing Partner, U.S. Center for Corporate Governance  
Innovation Leader, Audit & Enterprise Risk Services  
Deloitte & Touche LLP  
+1.617.437.2200  
[swagner@deloitte.com](mailto:swagner@deloitte.com)

### **Beth Kaplan**

Director, Audit & Enterprise Risk Services  
Deloitte & Touche LLP  
+1.714.436.7019  
[bkaplan@deloitte.com](mailto:bkaplan@deloitte.com)

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 150,000 people worldwide, Deloitte delivers services in four professional areas — audit, tax, consulting, and financial advisory services — and serves more than 80 percent of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the United States, Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP, and their subsidiaries), and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 40,000 people in more than 90 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's Web site at [www.deloitte.com](http://www.deloitte.com).