Deloitte.

SOX Optimization: Improving Compliance Efficiency and Effectiveness

Audit . Tax . Consulting . Financial Advisory .

SOX Optimization: Improving Compliance Efficiency and Effectiveness

In initially implementing the provisions of the Sarbanes-Oxley Act of 2002 (SOX), many companies faced serious dilemmas in striking a balance between complying with the regulations, keeping costs down, and attempting to garner benefits around improved internal controls. Many also sought to leverage the requirements to result in a competitive advantage and increased shareholder value.

Such concerns have been expressed by many participants in recent Deloitte[1] Dbriefs for Financial Executives webcasts and in the comment letters that registrants sent to the Securities and Exchange Commission (SEC) and Public Company Accounting Oversight Board (PCAOB) regarding the December 2006 Section 404-related proposals.

The SEC approved its final management guidance related to internal control assessments on May 23, 2007. The PCAOB approved its revised auditing standard for audits of internal control over financial reporting on May 24, 2007; the standard will be final when approved by the SEC. While the implications of the new guidance will vary based on a registrant's specific circumstances, generally speaking, companies should benefit from the fact that management will have specific guidance it can apply in its Section 404 processes. Further, the new guidance allows both management and auditors to focus on the areas of greatest risk. Additionally, the approved guidance includes significant investor safeguards, will preserve audit quality, and should help make Section 404 implementation more efficient.

For those companies attempting to attain compliance efficiencies *and* leverage improvement opportunities, a critical element lies in understanding the intersection of compliance management with performance management. Those companies that don't view Section 404 as a separate project, but rather embed compliance activities into ongoing operations, should attain superior results.

[1] 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.

The CFO's Quandary

The enactment of SOX placed great pressure on companies in general and CFOs in particular. During the first year, the demands to meet the basic requirements of the law meant that, rather than using SOX as a catalyst for business improvement, many companies struggled simply to comply. Out of necessity, some organizations focused on short-term results (compliance) rather than a long-term strategy (driving continuous improvement). Many SOX efforts lacked a consistent, methodical process. Companies had little inkling how to prioritize. This often created major expenses and many headaches.

In year two and subsequent years, the issue of cost landed on the CFO's doorstep. The perception: compliance was too expensive. The mandate: CFOs must cut costs. The quandary: how to reduce costs without jeopardizing compliance.

The resultant attempts to address this dilemma often lacked methodological rigor, and the outcomes were frequently unsatisfactory. In an effort to rein in compliance costs, many companies were stymied, uncertain whether they could safely cut controls, and, if so, unsure which controls to cut and which to retain. Efficiency and effectiveness in internal control over financial reporting was not attained.

Top-Down, Risk-Based Approach

A top-down, risk-based approach has been endorsed by the PCAOB and the SEC as a means to attain efficiency and effectiveness of internal control over financial reporting. A key component of this strategy is the understanding that not all risks, accounts, and transactions are equally important (a theme that we address in our Risk Intelligent Enterprise™ series of publications[2]). Also important are the principles that top-level, company-wide controls can have a more pervasive impact than lower-level, process-based controls; and that relevance and materiality should be key considerations in control testing plans.

How does the top-down, risk-based concept apply in the real world? Take payroll as an example. Because wages and salaries are typically a large expense item for most organizations, many companies have documented all of the controls within the payroll cycle, and are typically doing extensive testing of these controls, including sampling of individual transactions.

While there may be instances where this is an appropriate approach, for many companies applying a top-down, risk-based approach will reveal that payroll is highly routine, systematic, and predictable, is not subject to management estimates, and thus carries little risk of financial misstatement. When those "normal" conditions apply, then testing and documentation in this area can potentially be reduced by placing greater reliance upon management's periodic monitoring procedures.

Why Top Down?

Why focus on top-level controls? Because, like mountain snow feeding valley streams, everything flows from the top. Controls at the company-level can have an encompassing influence over controls at the process, transaction, or application level. Furthermore, controls that apply to all locations and business units help to set consistent standards and expectations across the company.

Company-level controls include items such as tone at the top; policies and procedures; codes of conduct; the assignment of authority and responsibility; management's risk assessment process. Also in this category are controls that monitor other controls, such as oversight and assessment of the internal audit function, the audit committee, and employee self-assessment and fraud prevention activities, such as whistle-blower hotlines, which can have an indirect relationship to financial statement misstatement risk.

In addition, many companies have the opportunity to significantly increase their reliance upon company-level controls that can directly mitigate financial statement misstatement risk, including controls over the period-end financial reporting process; monitoring controls such as analytical review and budgeting; and controls governing centralized processing, such as shared service environments.

[2] For more information on The Risk Intelligent Enterprise, visit www.deloitte.com/RiskIntelligence.

Deloitte & Touche LLP's SOX Optimization Approach

According to a February 2007 poll of Deloitte Dbriefs webcast viewers[3], almost 60 percent of surveyed companies plan to consider or revisit "control rationalization" as a result of the SEC's proposed guidance. A majority (53 percent) of companies are also considering changes to their testing strategy and levels of documentation as a result of the SEC's proposed guidance.

Deloitte & Touche LLP (Deloitte & Touche) believes companies should adopt a risk-based control rationalization approach as part of a larger effort towards SOX optimization. A key element of SOX optimization is control rationalization.

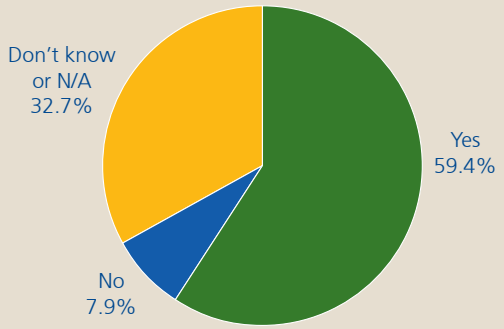
What, exactly, do we mean by "control rationalization"? Simply, we mean that not all controls are created equal. Some are more strategically important; some address more significant risks. Because of this inequality, controls should analyzed and prioritized, starting with the highest-level controls used by management to ensure reliable financial reporting . In conducting this assessment, the internal control and finance teams should pose a number of questions: What control objectives are addressed by these controls? Are they sufficiently detailed to provide the required level of assurance? What would be the impact of the failure of these controls? Is there sufficient evidence of the performance of these controls? By answering these and other questions, the team will be "rationalizing" the existing internal controls and better "aligning" their internal control structure with risk with the goal of retaining only the most strategic, efficient, and effective.

This approach focuses on the continuous process of designing and deploying only the most effective and efficient controls to address financial reporting risks. Control rationalization applies a top-down, risk-based approach; eliminates unnecessary controls; uses risk-based testing plans; and optimizes the design of company-level and automated controls.

It's important to note that because control requirements will change as the business changes, control rationalization should be approached as a multi-year, continuous effort that should be integrated into the company's operations. It can bring immediate benefits, but companies can achieve even more significant cost savings by adopting a long-term strategic approach to sustained compliance.

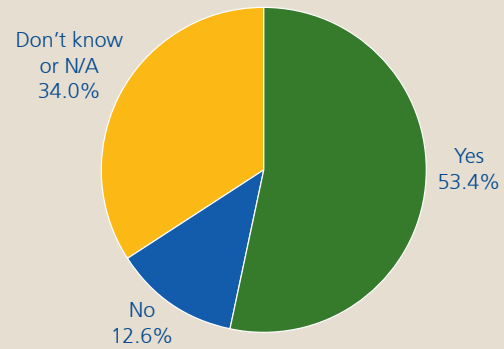
Does your company plan to consider or revisit control rationalization as a result of the SEC's proposed guidance?

Votes Received: 2426



Is your company considering changes to its testing strategy and levels of documentation as a result of the SEC's proposed guidance?

Votes Received: 2420



[3] The Feb. 9, 2007 Dbriefs for Financial Executives webcast was attended by 3453 business executives. The demographic breakdown included 45% manager level; 27% executive level; and 24% analyst level. Industries represented included financial services – 25%; technology, media, and telecommunications – 16%; consumer business – 13%; manufacturing – 12%; energy and resources – 9%; and life sciences and healthcare – 7%. Due to the fact that survey participants self selected, and thus do not represent a random sampling, the survey results are not statistically valid and should not be relied upon. Nonetheless, the data represents the collective thoughts and experiences of business people at scores of companies, and the accompanying interpretations are based on the experiences and the views of a number of partners and principals of Deloitte & Touche LLP.

Leveraging Technology

Effectively leveraging technology can help optimize a company's SOX effort in several areas, including the following:

1. Greater reliance can be placed upon testing of general computer controls and automated controls. In addition to helping management reduce its manual testing of routine systematic controls, increased reliance upon general computer controls and automated controls can allow management to focus its testing efforts in areas where changes have occurred or areas where there is greater risk due to non-routine processing, complexity, or level of judgment. At the same time, management can potentially reduce its effort in areas where the nature of the process or significant changes have not occurred.

2. Technologies can be leveraged to enhance the efficiency and effectiveness of management's testing efforts. This includes the use of file interrogation and continuous control monitoring technologies that can analyze entire populations of transactions for potential anomalies. These technologies can also help to augment management's anti-fraud programs and controls.

3. Technology can also be used to improve effectiveness and efficiency of management's overall compliance effort, including the following key areas:

    - Creating a common repository for all key elements of risk (including operational and strategic risk areas). Providing integrated, enterprise-wide support for all compliance and risk management activities.

    - Establishing a common repository for all controls-related documentation (including relevant policies and procedures).

    - Allowing for centralized capture of assessment and testing activities.

    - Providing automated support for management certifications.

Many organizations are still primarily reliant upon spreadsheets, Word documents, and, in some cases, manual efforts to support their SOX initiatives. In other cases, companies are using point solutions that are solely designed to support SOX compliance and are not integrated with the company's key financial systems. Such methods are unnecessarily primitive. In the last few years, the sophistication of compliance technology has improved dramatically.

In a March 2007 Deloitte Dbriefs for Financial Executives webcast[4] on compliance management, 49 percent of the surveyed participants said that technology tools are essential for the integration of compliance and performance. Attendees reported that the biggest challenge to integrating compliance within core processes lies in three areas:

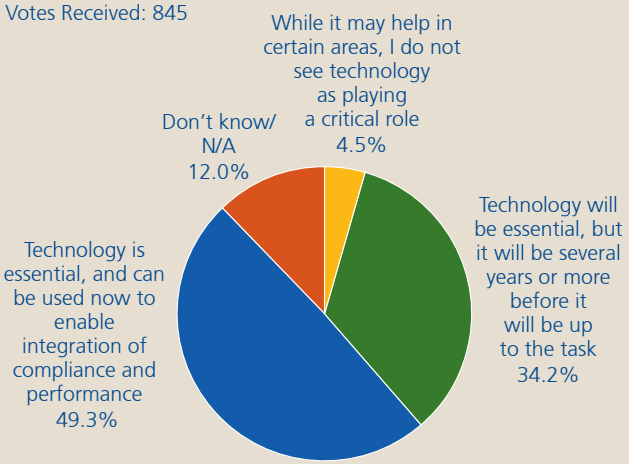
1) organizational resistance or inertia

2) lack of sponsor or champion

3) need for a compelling business case.

How do you view the role of IT in integrating the management of performance, risk, and compliance?

Votes Received: 845



[4] The March 22, 2007 Dbriefs for Financial Executives webcast was attended by 1213 business executives. The demographic breakdown included 43% manager level, 29% executive level, and 24% analyst level. Industries represented included financial services – 27%; technology, media, and telecommunications – 17%; consumer business – 11%; manufacturing – 12%; energy and resources – 8%; and life sciences and healthcare – 9%. Due to the fact that survey participants self selected, and thus do not represent a random sampling, the survey results are not statistically valid and should not be relied upon. Nonetheless, the data represents the collective thoughts and experiences of business people at scores of companies, and the accompanying interpretations are based on the experiences and the views of a number of partners and principals of Deloitte & Touche LLP.

Four-Phase SOX Optimization Approach

Deloitte & Touche has developed a four-phase approach to help companies optimize their SOX compliance work to achieve efficiency and effectiveness. The first two phases of this risk-based approach are tactical/short term. These phases can help the company generate immediate reductions in compliance costs and build a foundation for a sustainable internal control program. The last two phases go beyond the basic compliance requirement and may require a greater resource investment. But the payout can yield significant rewards.

Deloitte & Touche's SOX Optimization Approach includes the following goals:

- Understand the overall design and balance of controls and how they align with financial reporting risks.
- Shift focus toward higher risk areas to enhance compliance quality.
- Achieve cost savings by applying more efficient compliance efforts for routine processing-related controls.
- Identify how company-level (as opposed to process-level) controls can be improved to drive compliance efficiencies and reduce the organization's overall compliance risk profile.

Phase 1: Apply Top-Down, Risk-Based Scoping Approach Using SEC/PCAOB Guidance

This phase begins with a risk assessment to understand the company's financial reporting risks and to identify and possibly reconsider the design of controls. Through this process, companies can scope appropriate areas into the compliance program and develop a process where "in scope" areas receive the amount of attention commensurate with their level of risk.

Phase 2: Rationalize Existing Controls and Redesign Test Plans

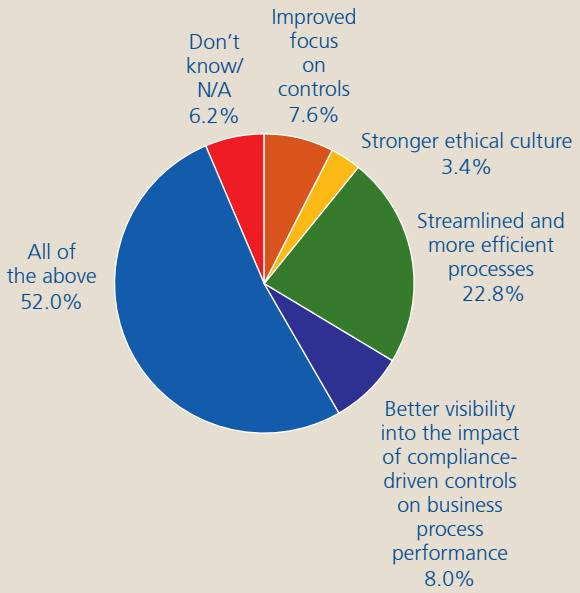
In this phase, companies rationalize both process-level and general computer controls; identify opportunities for enhancing control effectiveness; and consider removing redundant process-level controls from compliance testing. Phase 2 also involves applying a risk-based approach toward testing, which varies the timing, nature, and extent of testing based on the assessed risk. As a result, companies can direct their resources toward testing controls related to the highest risk areas, while minimizing the testing of controls in low-risk areas.

Phase 3: Leverage Automated Controls and Enabling Technology

In this phase, companies replace manual controls with automated controls (which are less prone to error and the potential performance problems associated with people-based controls). Automated controls can decrease costs and are usually easier and cheaper to test than manual controls. They also provide more reliability and can serve as monitoring controls. Continuous controls monitoring technology can be used in a number of business processes such as payroll, general ledger, purchasing cards, and travel and entertainment.

Besides cost reduction and assurance regarding compliance status, what do you see as the greatest potential long-term benefit to integrating compliance within core processes?

Votes Received: 962



Phase 4: Standardize and Centralize Processes/GRC Integration

The value derived from standardizing and centralizing processes and controls extends beyond compliance into day-to-day operational efficiencies. This phase focuses on integrating governance, risk, and compliance (GRC) activities in order to reduce costs, drive value, and improve overall risk management.

The payoff from standardizing and centralizing disparate processes and controls can be significant compared to the three earlier phases, although accomplishing this will be a lengthier process. A survey conducted during a March 2007 Deloitte Dbriefs for Financial Executives webcast validates this claim. Attendees polled during the webcast identified a number of long-term benefits derived from integrating compliance within core processes, including streamlined and more efficient processes, improved focus on controls, and stronger ethical culture.

Organizations that integrate GRC practices will discover it can be a key driver of shareholder value. However, this initiative requires strong leadership from the C-suite and the board. An integrated approach to GRC can help to improve the overall Risk Intelligence of an organization and enable the use of risk offensively, as opposed to defensively. This includes more effectively managing the risks associated with the critical operations or key strategic initiatives that are long-term value drivers.

Action Plans

Organizations need to consider the impact that the SEC's guidance may have on documentation, testing strategy, and design of internal control over financial reporting. The following are a few steps that can be taken in this direction:

1. Revisit risk assessment from a top-down, risk-based perspective. At the account and business process level, increase focus on the assessment of qualitative risk factors, such as subjectivity to estimates and nature of processing, as opposed to focusing primarily on quantitative factors, such as size of balance.

   Consider or revisit control rationalization. Focus on those controls that, should they fail, would materially impact the financial statements. Look first at company-level controls (especially those that directly relate to financial reporting risks) before focusing on departmental and process-level controls.

2. Recognize that your approach can and, in most cases, should be different than that of the auditor. Communicate with your auditor regularly through the process, but, in general, do not replicate his or her work. Determine in what areas the auditor can rely on your work, and where the auditor must test independently.

3. Increase the level of ownership within the organization for internal controls. Implementing a program of control self-assessments can significantly augment and enhance control testing work, while at the same time reinforcing the need for responsibility and accountability with the most important person in the control structure — the control owners themselves. Take some of the responsibility for control testing off the shoulders of internal audit, and imbed control testing and monitoring into daily operations. Deploy internal audit intelligently to maintain a balance of objectivity and ownership: management should get assurance from process owners; internal audit should provide reassurance in areas of greatest risk.

4. Focus on reducing effort. Investigate automated controls, which are generally more reliable, less costly, and more easily tested than their manual equivalents. Look for efficiency in control design.

5. Discuss revised plans and contemplated changes with the external audit team to help assess how these changes may affect the audit process.

Springboard to Improvement

A program of SOX optimization and control rationalization can help companies overcome the quandary of how to improve controls while simultaneously cutting costs — and do so without jeopardizing compliance.

Examples abound. In 2006, we authored an article in *Harvard Business Review* that illustrated the tangible benefits realized by several companies — including Kimberly Clark, PepsiCo, and Sunoco — that adopted a SOX optimization program[5]. More recently, we published an article in *CRO magazine*[6] that discussed the benefits of improving controls efficiency and quality.

Compliance with SOX and other regulatory requirements presents both burdens and opportunities. Forward-thinking companies will use the mandate as a springboard for taking an integrated, enterprise approach to Governance, Risk and Compliance, improving the overall Risk Intelligence of the organization.

[5] *Harvard Business Review*, "The Unexpected Benefits of Sarbanes-Oxley," April 2006. For a free copy, visit www.deloitte.com/SOX.

[6] *Corporate Responsibility Officer (CRO) magazine*, "SOX Benefits," March 2007: http://www.thecro.com/node/400.

Resources

For more information on Deloitte & Touche's SOX optimization approach, visit www.deloitte.com/soxoptimization or contact your Deloitte & Touche partner.

For more information on the concept of Risk Intelligence, visit www.deloitte.com/RiskIntelligence.

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

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

Dbriefs for Financial Executives

We invite you to visit 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

Dbriefs Webcasts Relating to Compliance and Sarbanes-Oxley

Section 404: What does the New Guidance Mean to You?
June 28, 2007

Governance, Risk, and Compliance: Evaluating Strategy, Structure, and Costs
May 24, 2007

The Next Stage of Section 404: Opportunities for Management to Optimize Efforts
April 26, 2007

The Intersection of Compliance Management and Performance Management
March 22, 2007

Extracting Lasting Benefits from Compliance Efforts
February 22, 2007

Special Edition Webcast Section 404: What do the Proposed Changes Mean to You?
February 9, 2007

CPE credits are offered to viewers of original live webcasts, but are not available for viewing archived programs.

Archived webcasts are available for 180 days after the live presentation.

#7230

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

Member of
Deloitte Touche Tohmatsu