SOX Monday Morning Quarterback – Lessons Learned and a Look forward

Mark Nelson and Keith Johnson
Protiviti Inc.

Introduction

On Monday morning it's easy to see what went wrong with the game plan. Hindsight is always perfectly clear. With Two years of SOX work now completed, it's easy to see where to make changes to your SOX game plan.

This white paper will provide practical advice and five key lessons to improve the SOX compliance effort. We will discuss moving from a manual Project based audit approach to an automated Process approach. We will also discuss how companies are using Continuous Controls Monitoring specifically for their Oracle E-Business Suite and PeopleSoft Applications to reduce their overall compliance cost.

Recent Changes

On May 24, 2007 the Public Accounting Oversight Board (PCOAB) voted to issue a final standard on auditing internal control over financial reporting (ICFR), as well as a related independence rule and conforming amendments to the Board's auditing standards. The new standard, Auditing Standard No. 5, *An Audit of Internal Control over Financial Reporting Performed that is Integrated with an Audit of Financial Statements*, supersedes Auditing Standard No. 2 (AS2).

The new auditing standard (AS5) is focused on maintaining the benefits investors have received from improved financial reporting. The new standard is intended to raise the auditor's "line of sight" by focusing the attestation process on obtaining reasonable assurance that a material weakness does not exist. The standard applies to all companies, irrespective of size, that need to comply with Section 404. Although the principles from AS2 have been retained, the PCAOB staff pointed out during the open meeting that the magnitude of change in the new standard should not be underestimated. These changes were focused on achieving a quality audit, consentient with the four objectives articulated by the PCOAOB in December 2007:

(1) Focus the internal control audit on the most important matters
(2) Eliminate procedures that are unnecessary to achieve the intended benefits
(3) Provide explicit and practical guidance on scaling the audit to fit the size and complexity of the company
(4) Simplify the standard

To achieve these changes, we have highlighted five Key Lessons to be discussed in this white paper.

1. Deploy a top-down approach to focus on what's important

A top-down approach still has not been applied in a manner that effectively reduces the extent and/or alters the timing of independent testing in routine processes with alternative sources of evidence. Management fraud most often has been perpetrated at the company level and in the period-end financial reporting process, and not within the upstream routine business processes. Despite that history lesson, most of the Section 404 compliance work is targeted to the process-level controls. There are at least three reasons for this costly incongruity:

First, the number of key controls is excessive, resulting in inordinate independent testing. While most issuers have reduced the key controls their personnel must test, many have more work to do. Second, company-level controls are more difficult to test than process-level controls. Because auditors generally prefer evidence from reperformance and inspection tests, they place more weight on process-level controls. Finally, management has not fully deployed company knowledge in setting the scope for assessment process. Management's assessment process remains substantially auditor-directed because of the focus on reducing external audit costs, and a reluctance to modify the compliance process when auditors conclude they must increase their testing if the modifications are put into effect. The result is that management is diverted to spend more time on less important matters. There are three steps managers should take: (1) Because the number of key controls to evaluate and test is the most important cost of the compliance process, companies should continue to refine their analysis of key controls to narrow them down to the vital few that really matter. (2) Managers should place more emphasis on evaluating company-level controls to reduce the extent and/ or alter the timing of independent testing of process- level controls with alternative sources of evidence. (3) Finally, when setting the scope of independent tests of process-level controls, management should fully utilize its knowledge based on its day-to-day involvement with processes and the underlying controls.

2. Consider qualitative and quantitative factors to implement a risk-based approach

Many companies applied a conservative approach in the initial year of compliance, and may have been overly inclusive of areas to evaluate and test. Because of the limited time available in the second year and the cost reductions made possible by the significant first-year documentation and remediation costs, many companies only updated their risk assessment for changes in the business, but did not take a hard enough look at the areas noted in the prior year as "high" or "moderate" risks to ascertain whether those determinations were still appropriate.

Last year, the PCAOB staff indicated that "quantitative measures alone are not determinative as to whether an account should be identified as significant." Since that guidance was issued, significant traction in applying it in practice has not occurred. In addition, the audit process is largely focused on applying quantitative measures of account-level materiality, which was another point of debate during the roundtable. The PCAOB is likely to address these and other related matters in amending AS2 so that qualitative and quantitative factors comprise the total mix of information that is available for determining the significance of an account and the nature, timing and extent of tests of controls.

It is our experience that management considers qualitative as well as quantitative factors when assessing risk. An effectively coordinated companywide risk assessment process offers an opportunity to reconcile management's perception of risk with that of the auditors, and vice versa, and should be encouraged as an approach to initiate constructive dialogue between the parties. If testing continues to be conducted in areas where, in the view of management, the risk of material error or fraud is relatively low, management should refine the prior-year risk assessment by giving more explicit consideration to supplementing the quantitative materiality factors with qualitative factors, e.g., the nature and significance of possible error or fraud that could occur in an account (i.e.,"what can go wrong"), the susceptibility of an account to error or fraud, the robustness versus subjectiveness of the processes for determining significant estimates, the nature and effect of related party transactions, and the testing experience and problem areas from prior years that may require attention during the current-year assessment. While the external auditor's expectations and requirements will continue to influence the scoping of management's assessment process, qualitative factors should at least be considered when planning the nature, timing and extent of independent testing.

3. Optimize IT Controls to increase cost-effectiveness

Use of automated IT controls remains an area of "mystery" to many management teams and sometimes to auditors as well. The cost of relying extensively on manual controls in sophisticated financial reporting processes never has been as evident as it is today. Not only do manual tests of controls by companies and their auditors require much time and effort, they are not always reliable in sophisticated environments. The costs inherent in this labor-intensive compliance approach are incurred each year until management reevaluates the controls portfolio with an eye towards balancing the mix of automated and manual controls to increase controls cost-effectiveness. Because an automated control takes substantially less time to test than a manual control, the savings can quickly add up. For example, manual controls require an inspection of each sample occurrence, often embedded in reams of documents, whereas an automated control only requires a one-time observation of either an application's performance or an ERP configuration setting, provided it is designed, maintained and secured effectively. Testing of a remediated manual control requires additional sampling versus the real-time resolution and retesting of an online control.

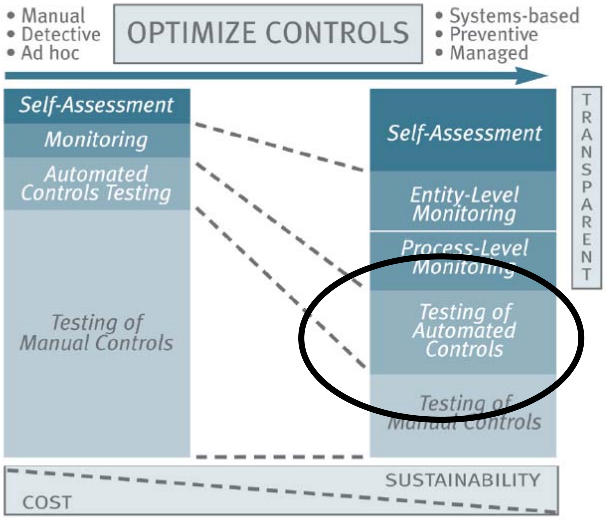

Figure 1 – A balanced test plan

Control automation can provide significant benefits to most organizations. Some examples of these benefits include: (a) Decrease in employee time conducting or supervising tedious manual controls, (b) Decrease the cost of annual assessments through replacing slow, manual error-ripe testing with the far more efficient observation of an on-line setting, (c) Reduction in the odds of human error and fraudulent manipulation through forced on-line consistency and compliance, (d) Increase in quality and reduction in re-work by detecting problems quicker and emphasis on preventing them altogether, and (e) Proactive management of audit fees by applying the same logic of test savings to external audits and achieving increased auditor reliance on internal testing of safer automated controls. There may be resistance to change from tired compliance teams that are just getting comfortable with the existing internal control structure. However, the opportunity for long-term savings is too great to ignore, not to mention the need to respond to increasing pressure from external auditors to rely more on automated controls. Therefore, a fresh study of automation opportunities should be carefully considered to maximize ongoing value and avoid competing against companies with a lower cost structure. Failure to automate in high-value areas may institutionalize a high-cost internal control structure built on excessive reliance on inefficient manual controls.

4. Improve operational effectiveness and efficiency of upstream processes

Most of the cost increases from Section 404 compliance are internally driven. According to Table 8 included in Appendix I of *The Final Report of the Advisory Committee on Smaller Public Companies* to the SEC, the audit and audit-related fees increased for accelerated filers in 2004 by approximately 50 percent over the prior year. A study by AMR Research (AMR) points out that costs incurred by companies, inclusive of external audit costs, increased by more than 100 percent during the same period. A more recent AMR study of larger companies noted that only 19 percent of financial executives report their companies realized the cost savings they expected during 2005. This conclusion is reinforced by a recent Financial Executives International study that also indicated cost reductions in 2005 fell below expectations. Thus, many companies have expressed, and continue to express, the view that Section 404 compliance costs need to be reduced by making the compliance process more cost-effective.

A significant portion of the total cost of financial reporting lies within the upstream business processes that initiate, authorize, record, process and report routine transactions. These processes include procure-to-pay, conversion, order-to-cash, capital expenditure and treasury, among others. As companies begin to understand that high compliance costs are largely a result of high-cost transaction processes, they see opportunities for: eliminating redundant activities, platforms and other nonessentials; simplifying and standardizing processes: centralizing common and similar activities: improving the mix of automated and manual controls; and transforming inefficient "detect and correct" controls to preventive controls that "build in" versus "inspect in" quality. As processes are improved to address these opportunities, the better mix of controls will lead to more efficient controls testing for both the company and the external auditor.

Many companies are seeking to optimize their compliance costs through improved "filtering" of the controls population to evaluate and test only those controls that matter. While this strategy is sound, it has just about run its course for many accelerated filers who have completed their second year. If there isn't a strong focus on improving the capability, transparency and operational performance of financial reporting processes, and on strengthening company-level controls and monitoring processes, companies will end up planning their Section 404 compliance activity for subsequent years around a high-cost internal control structure. This compliance activity will likely continue to emphasize heavily the minutiae of detailed manual testing of routine process-level controls.

While we agree that the conversation around "pass-fail" and managing external audit costs is important, we believe that this conversation can only go so far in gaining traction as to improving compliance cost-effectiveness. In Years Three and Four, the Section 404 conversation should focus more broadly on "process capability," as determined by the quality, time and cost performance of the upstream business processes as well as the extent of financial reporting risk sourced within those processes. Companies choosing to deploy the transparency provided by Section 404 compliance as a means to improve the quality of their upstream financial reporting processes, and institutionalize the compliance process around high-quality financial reporting processes, are experiencing further reductions in their compliance costs. What's the message? Management should get the company's internal control structure in order by directing attention to improving the operational efficiency and effectiveness of upstream financial reporting processes, including the underlying internal controls embedded within those processes. By taking that approach, companies not only drive down internal processing and management assessment costs, they also are able to reasonably expect external auditors to align their approaches with the more effective design.

5. Don’t wait on Washington to act

As previously discussed, the SEC’s management guidance and the revised Audit Standard are now completed. Implementation timelines are expected to extend into 2008. However, companies that act now can plan and implement their improvements over time, avoiding a “large project” to reap the benefits. The message: Management should focus on doing the right thing in applying the above lessons, and should not wait for the SEC and PCAOB to act or continue with future changes.

Transitioning from Project to Process

According to a recent survey by Financial Executives International (FEI), 85% of CFO’s believe the costs of Section 404 compliance outweigh the benefits. Clearly, change is required to reduce the annual cost of complying with Section 404, increase the value to the organization from compliance activities or both. We call this change from an initial, ad-hoc environment to a sustainable environment “Project to Process”. The Project to Process approach is comprehensive, reflective of the guidance emerging from the SEC and the PCAOB, and is designed to reduce compliance costs over time while increasing process performance by building in quality within financial reporting and upstream business processes.

Because a company’s ERP system typically processes a large majority of the financially significant transactions, the need to have strong internal controls embedded within the ERP to ensure data integrity is high. The good news is that major ERP systems are delivered with significant and growing capabilities to enforce internal controls and security within the application. The bad news is that for the majority of companies who implemented their ERP prior to 2004, internal controls and security in the context of Section 404 was not a high priority. Due to a lack of time and resources, companies tended to document manual controls in their first year of compliance. Manual controls were more familiar and better understood by both external and internal auditors. However, the number of manual controls tested is the single biggest driver of SOX compliance costs. As depicted in Figure 1, companies need to balance the mix of manual controls, automated controls, monitoring controls and entity-level controls to achieve the most effective overall controls environment. For most companies, that means increasing the reliance on automated controls with a corresponding reduction in the number of manual controls tested.

Getting Started

So what should companies do? First, Attain, then Maintain. In the Attain phase, the company will optimize the automated control environment. To move a control structure and the associated testing toward reliance on automated controls takes time. It will require input from a variety of internal business constituents and at least some technology investments. In this regard, organizations should begin by examining the sources of evidence supporting management's conclusion as to the operating effectiveness of internal control over financial reporting. This examination should ordinarily drive efforts to start rebalancing the automated controls portfolio.

The effort begins with a fresh look at the organization's current key controls, with an eye towards several factors. We have found controls automation efforts to be most successful in yielding value-added benefits when they are: (a) applied through an integrated solution (e.g., ERP), because the improvements have a multiplier effect across common processes, (b) used to replace manual controls that are particularly expensive to operate and test, (c) utilized in risk areas that have the most impact on reports and performance if controls fail, (d) employed in areas of heightened external audit sensitivity, such as segregation of duties, an area of concern to the audit firms, (e) directed toward current practices that are more prone towards error and breakdowns, and (f) operated in association with procedures that are repetitive and require little judgment or human intervention. Applying the factors above to manual or poorly automated controls can help prioritize management's options for automating or optimizing controls.

Pre-requisites to relying on automated controls include sound program and configuration change management controls as well as strong security controls. If either of these general controls is weak, automated controls are vulnerable to override by management and other personnel. In addition, the compliance team would be unable to prove conclusively that the automated controls remained intact through the end of year.

Management should begin by taking stock of the existing application controls. In Year 1, configurable application controls were typically documented and evaluated separately from manual controls, often near the end of the effort. These controls need to be considered together to determine if a control objective can be achieved by the automated control(s) alone. In some cases, a change to the configuration is necessary to strengthen the design of the automated control. The controls and resulting process changes must be documented, tested, and implemented under a change control process.

Similarly, application security, particularly user access to powerful authorities and segregation of duties (SoD), was often evaluated late in the game. Many companies have security administration processes that require approvals for adding a new user, but often management did not explicitly define incompatible duties nor define who should have powerful authorities. As a result "problem profiles" were implemented, and often spread throughout the system. The first key activities to Attain an appropriate application security environment is to define the "rules" by which application security will be evaluated, and then evaluate the current user base to determine the number of violations. The use of an automated tool to perform the analysis can greatly speed up the process. SOD issues take two forms. In the first, a conflict exists within a single profile or role (intra-role). Each user assigned this role results in a conflict. The second type of SOD issue results from a combination of roles that together have incompatible duties (inter-role). Both types of conflicts should be evaluated, but often cleaning up conflicts within a role represents the low-hanging fruit that can quickly bring down the number of violations present in the environment. In our experience, most companies cannot completely eliminate SOD conflicts from their environments. However, the removal of unnecessary issues typically represents a majority of the total population of issues.

The Attain phase typically represents a significant investment of time and effort, with the promise of annual savings once the compliance testing approach is adjusted to reflect the new environment. However, controls are needed to make sure the new environment is Maintained. Testing of security and application controls represents a point-in-time analysis of how the system is configured today. The auditor's next question is "How do you make sure that configuration was effective all year?" This is where the IT General Controls (ITGC) associated with security administration and change control come into play. The IT department typically establishes ITGC processes, but the traditional general controls often are not designed appropriately to address ERP configuration change control and application security controls (such as SOD). Therefore, new capabilities are necessary to manage these risks. These additional controls capabilities can be thought of as Continuous Controls Monitoring.

Implementing Continuous Controls Monitoring

Maintaining an effective automated controls environment over time requires monitoring to ensure that key controls remain in place and that changes can be identified, evaluated and corrected, if necessary. Over time, employee turnover, poor change management and other factors may decrease the effectiveness of the automated control environment. Without active maintenance, companies with a strong automated control environment may eventually fall back into the “project” mode of compliance to bring the control environment back to a high level of effectiveness.

Continuous Control Monitoring (CCM) allows companies to monitor security in near-real time, and in some cases, can enforce required approvals before a user with security conflicts is provisioned. Other features of continuous controls monitoring include configuration change management, real-time transaction exception monitoring and master data change alerts. These features keep management on top of, and in many instances, ahead of developments. They can immediately detect problems or often anticipate and avoid them. Collectively, these automated capabilities can help to enable a company’s monitoring controls for preventing/detecting fraud which is highlighted in the new guidance from SEC and PCAOB.

A story about a Protiviti SOX client illustrates the effectiveness of these tools. Company A had been through two years of SOX compliance when Protiviti was asked to assess the company’s high-risk control areas. The findings fell into four categories: First, 40 controls were tested without exception. The potential for improvement here resided in the ability to replace manual testing with automated testing. Second, 69 controls were tested with exception, meaning the company was improperly relying on these controls. Third, 98 controls were enabled, but were not documented, tested or relied upon. As a result, this company missed an opportunity to place more reliance on these controls to reduce manual testing. Finally, 145 controls that could have been implemented were not enabled by this company. One conclusion to be drawn from this example is that prior-year testing conclusions may have been wrong due to the limitations of manual testing of sophisticated applications.

Another trend we see is external audit firms deploying testing tools to automate their own testing and achieve increased coverage. This may provide management another incentive to employ their own automated tools to transition from project-to-process is the stance of the external audit firms.

A number of new Continuous Controls Monitoring software solutions have entered the market over the past few years to enable automation initiatives. Leading solutions include Oracle Internal Controls Manager (ICM), Logical Apps ACTIVE Governance and Approva BizRights. However, it should be noted that automation is not appropriate for all situations. As always, there should be an evaluation of the holistic cost of automation verses the value of future savings and increased quality and effectiveness of the internal control structure.

Conclusion

When a team loses the big game, a great coach always reviews the game film and puts forth a plan to address the problems. The SEC and PCAOB have done the same, with their new guidance based on the results of multiple years of SOX. The message is clear, apply a top down approach to focus on what is important, consider qualitative and quantitative factors to implement a risk based approach, optimize IT controls to optimize cost effectiveness, improve operational effectiveness and efficiency of upstream process and don’t wait for Washington to act. Will your company be heading to the all-star game, by following the coaches new game plan?

This white paper was adapted, in part, from Issue 8, Volume 2 of The Bulletin, *a periodic newsletter from Protiviti that focuses on key corporate governance and risk management issues impacting companies today, and from Protiviti’s* Guide to the Sarbanes-Oxley Act: Managing Application Risks and Controls.