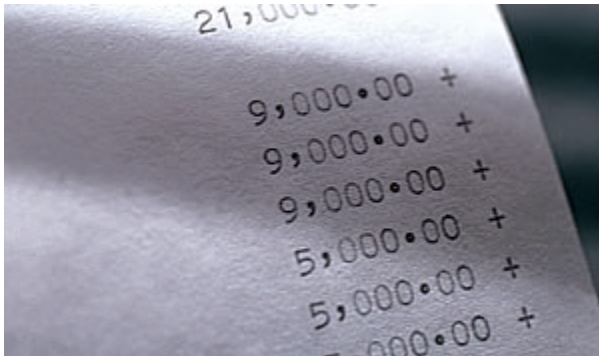


BOTTOM LINE

# COMMON-SENSE SOX

The best practice today in Sarbanes-Oxley compliance might be risk-based auditing. Find out why. **By David F. Giannetto**



Sarbanes-Oxley (SOX) compliance – year two. Organizations have come to two universal conclusions: Initial compliance costs cannot be sustained despite ongoing requirements, and the work done to comply must be leveraged to provide a value that the market will recognize.

The high cost and non-value-returning efforts of SOX compliance also are raising concern among non-accelerated filers and not-for-profit organizations.

Collectively, the market is screaming, "There must be a better way." The growing light at the end of the tunnel is a risk-based approach that applies a voice of reason to the audit and compliance process.

## Standard Approach

The original approach to SOX compliance took the standard internal auditor approach and applied it to the financial statement. Because the standard internal auditor approach audits and accounts for every detail in the process under review, the approach essentially required this level of scrutiny for nearly every process within the organization.

Perhaps it was the best approach available at the time, but when viewed from the higher perspective of the overall organization, it is clear that this approach could not stand the test of time. Despite the need for sound fiscal management, the requirements for businesses to generate revenue, profit and customer value – the three true measures of success in business – will, for good or bad, in the end always dictate the approach that the organization can afford to take.

Surprisingly, risk-based auditing agrees with the internal auditor's process by which compliance is reached; it simply seeks to apply it to those areas that truly create risk for the organization. This means that not all areas should receive equal attention and scrutiny, but that the attention should be based on the actual risk created by the process itself.

Payroll, for example, is one of the highest-expense items for almost every organization, yet it generates little risk. Payroll expenses remain fairly constant over time, with increases and decreases clearly related to headcount and salary changes. Often the payroll process itself is outsourced, adding another layer of third-party controls to the process.

Several relatively simple mathematical checks can serve to provide high-level assurances that there will be no material misstatement carried forward. Therefore, this area does not require the scrutiny that gray areas, such as accrued revenue, would. This is, after all, the basic assurance that SOX seeks to provide the shareholders.

Even an act as sweeping in its changes as SOX cannot remove risk from business. Business is,

after all, risky. The risk-based approach accepts that risk will always remain and does not seek to remove it – what amounts to a time-consuming, profitless endeavor in most situations.

It seeks to quantify and control it to the extent possible, which is something very different. Applying less scrutiny in lower-risk areas within the organization reduces the overall expense associated with SOX compliance efforts but, unfortunately, still does not create a return on investment.

To comply with the "if-you-didn't-document-it-you-didn't-do-it" approach mandated by the Sarbanes-Oxley Act, organizations must, typically as a first step, define the processes within the organization that impact the financial statements. This is most often done through process mapping. It is the resulting process maps, or narratives, that provide the opportunity to realize a return on investment.

Under the current approach, internal auditors use these maps as a means to define key processes and identify key controls within them. The typical internal auditor focuses on the process controls, with little regard for the effectiveness or efficiency of the processes itself.

Although it may be a stretch to ask members of the typical internal audit group to utilize these process maps for any other purpose than what their training and experience have so far asked of them, they do tell a great deal to those who have the training to use process maps as the first step in improving the efficiency and effectiveness of internal processes. They become the very foundation of process-improvement efforts. For organizations seeking to undertake a process-improvement initiative, the first step is often creating process maps for the processes under review. SOX has already done this for them.

### **Value Chain Focus**

The main difference between process mapping to identify key controls and process improvement is that process improvement efforts focus on the value chain. An output from one process becomes the input, or the trigger, to begin the next process. This process then uses the input to create something new – the new process adds value. The result then becomes an output and the chain continues.

If an output is not needed to trigger a new process, then the process that created it may not be needed and becomes a candidate for process improvement. A simple example for most organizations would be the excessive number of reports that are generated – often a time-consuming manual process – that are then distributed and never used as a decision-making tool. The recipients never find value in them; therefore, they are unneeded.

Process improvement and internal audits are clearly two separate schools of thought and require two separate skill sets to be effective. To leverage these process maps and the work that has already been done, the organization could assign a multi-functional team to the original creation of the process maps. A team comprised of both internal auditors and internal or external business consultants creates process maps while also identifying ineffective or inefficient processes throughout the organization.

The internal auditors then focus on internal control issues while the consultants focus on areas of weakness to understand why a process has been created, and either undertake the improvement effort themselves or assign it for improvement by those responsible within the organization.

If the organization has already created process maps, these can be reviewed by someone with experience in improving processes to identify suspect areas. These areas are then likely to require a small amount of additional investigation to determine if the suspicion was in fact warranted; if so, the same improvement effort then takes place.

The amount of effort required to bring the SOX process maps up to the additional level of thoroughness required for process improvement is well worth the effort. If not, these process maps, and the work done to produce them, will provide relatively little concrete return for the organization.

### **Significant Change?**

It remains to be seen whether or not this change in approach will mark a significant change for the actual role that internal audits play within organizations. Traditionally, they have never had a responsibility to provide a tangible return for their efforts. Non-public and not-for-profit organizations are already requiring more from their internal audit group and expecting them to go beyond standard, public practices. The extension of their efforts crosses into the realm of process improvement because it is the shortest path to a return on their efforts.

In addition, for these organizations, the internal audit group is often the most knowledgeable about how many processes are performed and how they interrelate. The diverse requirements of these environments broaden the skill set of these auditors and more readily prepares them for newer approaches such as risk-based auditing.

Nearly every organization subscribes to the theory of continuous improvement. Although far fewer are actually able to embrace it, the ongoing process review and signoff required by SOX can actually put in place the ongoing review process needed to drive this initiative. It is an approach that, when viewed at the higher perspective of the overall organization, makes better business sense than the current approach.

Surely, the SOX compliance process will continue to undergo additional change. But one thing is certain: Organizations, even those only choosing to comply with SOX as a best-practice approach, will continue to spend a significant amount of their revenue on compliance efforts. Today, that best-practice approach is called risk-based auditing. **USBR**

David F. Giannetto is director of enterprise performance management for Cohn Consulting Group. He can be reached at [dgiannetto@jhcohn.com](mailto:dgiannetto@jhcohn.com) or 973-871-4037.