

<http://www.itcinstitute.com/display.aspx?id=242>

Gap Traps: Closing the Loops in Compliance Coverage

Are there obvious elements that companies are missing in their compliance efforts?

By Linda L. Briggs

With the flurry of activity around regulations and another window of Sarbanes-Oxley compliance closing in, are there obvious elements that companies are missing in their compliance efforts? Are there common weak links in security, storage, documentation, or testing? Are there process gaps where departmental compliance efforts just aren't connecting? What exactly are companies failing to include in their SOX equations? To answer those questions, the IT Compliance Institute spoke with **Glenn G. Wisegarver, a senior manager at Hitachi Consulting**, which provides business and IT consulting services, including compliance-specific assistance to companies worldwide.

Can you point out some specific areas where companies might identify gaps in their compliance coverage?

First of all, everybody's auditors, regulators, corporations themselves, is still learning what compliance looks like. This will be an iterative process over time. As understanding is gained, there will be more common agreement about what compliance looks like.

With respect to gaps, I'll focus on the technology area. First of all, there's a huge variety of regulations and standards out there [already]: SOX, privacy regulations at the state and federal level, HIPAA, Basel from Europe, and many more. One of the key gaps, and this is going to be a difficult one for companies to resolve is, integration between all these compliance standards into a single unified framework that actually works, as opposed to more piecemeal compliance efforts. That's a very significant gap.

Another gap that I frequently see is what I'll call the connection points between business process, business process owners, the technology controls, and the associated IT organization. There tends to be, in many, many companies I see, a figurative wall between business organizations and functions and the IT organization.

When one looks at business processes, it's really the thread that goes through both the functional areas as well as, technology processes. Yet, at the same time, the gap is that the functional side and the IT side don't necessarily talk to identify all of the things that need to be included [in] the compliance process. That's a definite gap.

Those are higher-level gaps. Another area where I frequently see specific gaps has to do with access controls and [their] management. That's access by people to a variety of [processes and data], as well as their roles and rights. The gap here tends to be this: Companies fail to realize that there are really three system layers to consider: The first is the operating system, because there are controls around most of the operating system technologies. The second is the broad

network, which some companies refer to as the infrastructure layer, and access associated with that. The third is the application layer itself and the variety of applications running there.

All three of those technologies typically have access controls, but what I frequently see is a focus on just the network layer, for example, the operating system layer and the application layer don't come under the same standard of control.

But these three all touch each other. For example, it's fairly common that when a person leaves a firm, a certain level of access rights are taken away quickly, based on a fairly well developed process. But many other rights, either to applications or in the operating system, aren't necessarily taken away. It's fairly common for a lot of gaps to be seen there.

Another area where I see gaps is access [rights] between production and the development environment, usually having to do with source code [and] developers. It's most commonly in database environments, because that's one of the environments that developers touch frequently. Typically, one of two things happens: Either this position and responsibilities isn't recognized, or second, it's recognized, but the resource pool is so small or specialized that the company chooses to simply ignore it, or doesn't recognize that you have this concentration of duties. Thus, there's a weakening of controls in [a developer] having access to both.

It sounds like many of these issues have to do with security.

Yes, some of it is security-related. Along those lines, another area, and this is debatable as far as direct applicability to financial reporting processes and systems' has to do with disaster recovery and business continuity.

I think most companies are at least reasonably good at backing up. But the gap is, they never test the system to make sure it works. The time to test is obviously in a safe, unhurried environment, but that testing component falls short. From a business continuity perspective, which obviously is much broader than the technology itself, the planning is not there. If the company actually did have to respond and resurrect things, they simply don't know how to do that. I would say that tends to affect more midsize and small companies. Large companies tend to have better organization, planning and processes around business continuity and disaster recovery.

So that's not just Sarbanes-Oxley, for example. That's also a broad business continuity issue.

That's right. Many of these end up touching a number of other issues.

The last area I'll mention has to do with actual compliance activity itself. All of these things we've talked about and beyond need to be tested by the companies themselves as part of the management self-assessment. The challenge here is, many companies are asking not auditors, but their own internal staff to do that testing. Many of these people don't really have the internal control background to know what appropriate testing looks like.

So the gap comes when the individual firm tries to test based on their best efforts, but it doesn't meet the standards needed to actually attest to whether [they're in] compliance or not. So they end up in this iterative cycle where somebody either external parties or their external auditors, says, "Your testing isn't sufficient; you have to do it again. Yet, at the same time, in the example of the external auditor, they really can't tell you how to do it, because then you start to run into a conflict of interest.

Given that sort of gap in internal knowledge, what should a company be doing instead?

In terms of internal testing, companies need to develop a clear picture of what compliance looks like within their firm, with as much detail as possible. They need to assess what their testing requirements are going to be, then actually establish a training program for the people who are going to be doing the testing.

For companies where the testing is done part-time, the training becomes a very critical element. If companies aren't willing to put together a training program, then essentially they're pushed into a situation where their own people are forced to hire outside expertise to help them.

What about addressing some of the other compliance gaps that you've mentioned?

Broadly speaking, companies need to come to a decision about what compliance looks like for them. That's especially true for those companies that are moving into that window of compliance, as with Sarbanes-Oxley. They really need to approach this from a project perspective, at least the first time. They also need to start early, as opposed to waiting until their backs are against the wall, which is another common problem I see.

Begin by establishing a project with a set of deliverables. The first set of deliverables comes around definition: what does compliance look like, who's required within the firm to comply, what processes are covered within that scope, what level of testing is needed, and what are the roles and responsibilities around that?

What about tools and technologies that can help? Are there useful products that companies can be adding to plug the gaps?

There are two answers to that, beginning with a company's existing technology infrastructure and the applications that they have today: Companies need to realize that their ERP systems, CRM systems, decision support systems, supply chain management and so forth those applications usually have controls available to be implemented.

A CIO of a rather large business unit [asked me,] Should I wait for the next generation of business applications, so that all the new controls will be in them? I said, I wouldn't necessarily wait, because the revolution isn't going to happen. For the most part, those applications already have a robust set of controls available to be implemented the Oracles and the SAPs and the Hyperions and the Cognoses of the world

aren't going to make revolutionary changes to their products. They don't really need to the controls are already there.

What you will see in software has to do with [things like] document management, because if nothing else, Sarbanes-Oxley and a lot of these other regulations require a tremendous amount of documentation. That needs to be managed so that [employees], as well as the external auditors, can find the documentation.

Another area is the risk assessment piece of the internal control environment. There are applications out there today, and most of them fairly immature, but over time I expect those to mature and become more useful.

What companies need to understand, at least at this point, is that there's no silver bullet. There's no single application that's a compliance management application, that does all the things that management thinks needs to be done right now.

I think companies are indeed looking for that compliance silver bullet.

Oh, very much so, I hear it all the time. Tell me what Sarbanes-Oxley tools there are, they ask me, and they're expecting a short list of three products so they can choose one. Unfortunately, that's just not the case.

Companies need to realize that to try to put all of those technologies together into one application would be a monumental feat. It may happen over time, but it's going to be slow.