Information Technology Compliance: Past, Present and Future

Information technology compliance activities have evolved rapidly over the past decade. To help define the future of IT compliance, a look back at early efforts, combined with observations on today's activities, is presented in this article.

**A BRIEF LOOK BACK**

Historically, IT departments' roles in compliance (figure 1) was point-in-time focused or based on some significant event. Compliance efforts did not consider IT risk management as an umbrella framework or these efforts as part of a broader enterprise-wide compliance function. Remember the ramp-up to Y2K? The mad rush of IT consultant and auditor activity to ensure that Y2K considerations were addressed in enterprise systems was the ultimate illustration of a one-time compliance pandemonium. Other regulatory requirements and audit activities such as industry-specific certifications (e.g., Payment Card Industry [PCI] standards) or support for a service provider function (e.g., Statement on Auditing Standards No. 70 [SAS 70] reports) have also been around for some time, but were typically tackled as an annual project and by a narrow set of individuals within IT.

Why was this so? The compliance framework for IT was focused mainly on the engineering, testing or build-related processes of developing applications, following either the Software Engineering Institute (SEI)’s framework or ISO 9001 as the basis for compliance. This was mainly attributed to the customized nature of enterprise systems, whether purchased and modified significantly, or developed completely in-house. This set of activities usually fell within a specialized group within IT and its coordination did not significantly impact the broader organization. Also, enterprise compliance was typically a set of activities that others in the organization cared about. Finance, legal and human resources had always had sustained compliance functions that they managed on an almost daily basis.

IT compliance has come a long way over the past decade. This is especially true in the years since the Sarbanes-Oxley Act of 2002 burst onto the scene and gave public company IT departments their first real taste of playing a significant role in complying with a major enterprise-wide regulatory requirement. For the first time, corporate executives were forced to view IT as a critical link for compliance success and IT staffs were educated on a rigorous set of control activities that must be designed, operated, tested and audited.

Mike Pearl, a partner in PricewaterhouseCoopers’s advisory practice recalls, “In the late 1990s, comprehensive IT compliance programs were not even contemplated. Rather, IT reacted to specific compliance requests and usually in a fairly disorganized manner.”

That was then, this is now. What do IT compliance programs look like in today’s public companies?

**IT COMPLIANCE TODAY**

As the world has moved away from custom applications to noncustomized packaged and managed applications, including Software as
a Service offerings, the emphasis has been placed more on
the change control and the operational activities required
by IT. Coinciding with this movement was the introduction
of the Sarbanes-Oxley Act, specifically section 404, which
forced companies to formalize controls over the production
environments and shifted the burden from the build function
to the run function. Arguably, the Sarbanes-Oxley IT
general controls requirements have had a direct effect on the
increasing success rate of IT outsourcing initiatives. With
clear policies, standards and process controls in place, the
ability for a third-party service provider to deliver services that
meet predefined service level agreements (SLAs) as well as to
demonstrate effective controls to an evidentiary standard has
improved dramatically in the past five years.

At the same time, annual assessments for PCI and SAS 70
compliance have become mostly routine, changing only when
business processes change or when merger, acquisition and
divestiture actions are impacting the technology environment.
For most accelerated filers, Sarbanes-Oxley compliance
has matured and become routine as well. Public Company
Accounting and Oversight Board Auditing Standard No. 5,
which updated the original Auditing Standard No. 2 in May
of 2007, relaxed some of the rigor around the impact of IT
general controls on the overall Sarbanes-Oxley report. It
helped some tasked with IT compliance to scope out some of
the lower-risk IT systems and controls that were less directly
linked to accurate financial reporting.

With a new sense of compliance confidence and
experience, a variety of IT compliance models emerged to take
on other areas of regulatory requirement. The most mature
model is the one that has fully adopted an IT department
ownership role of technology compliance efforts for the
organization. The IT leaders consider compliance functions to
be high priority for the department and organization overall
and back that philosophy with resources and funding.

Another model, a “hybrid” model, is one where internal
audit, IT and others in the organization share responsibility
for IT compliance. This model usually results from the lack
of a strong compliance organization within IT or an internal
audit department that is unwilling to let go of its role in
IT compliance. This model is probably the most prevalent
in today’s organization and is a holdover from year two or
three of Sarbanes-Oxley. In this model, there may be a few
employees in the IT department who understand compliance
and may want to take on a greater role, but lack the resources
or executive-level commitment to grow the compliance
function within IT. This model has the opportunity to

With the positive progress made by the organization
described, some IT compliance efforts have made little progress
in their maturity since the advent of compliance requirements.
They continue to be reactive and fail to take advantage of any
of the significant lessons learned over the past 10 years. In this
model, the corporate internal audit function may be overseeing
compliance as part of its overall annual audit plan and utilizing
IT only in a “subject matter expert” capacity. IT usually views
these compliance requirements as a necessary evil, distracting
the IT department from its primary duties. Compliance
activities in this model are viewed as adding little value to the
organization overall.

Other models exist depending on the enterprise’s size, its
regulatory compliance maturity and executive sponsorship
of IT compliance initiatives. A strong overall corporate risk
management function will sometimes enable IT to develop
its own program, but comprehensive IT risk management
programs are still immature in most public companies today.
Beyond theory and into practice, a survey was conducted
in 2007 of IT and business leaders. The survey sought to
gather empirical evidence on the perceptions of an alignment
between IT and the business as a result of compliance
efforts overall and specifically Sarbanes-Oxley efforts.
The results of the study revealed that 63 percent of
business leader respondents and 85 percent of IT leader
respondents believe that compliance efforts, in general,
have moderately or strongly influenced greater alignment
within their organizations.2

In a webcast titled “Competitive Advantage Through
Compliance: Making Sarbanes-Oxley Work for You,”
the presenters discuss how much the legislation has cost
companies to implement, and also what advantages above
and beyond compliance can be achieved. Specifically, they
state that the other benefits achieved are through efficiency in
“tightening up infrastructure, including separation of duties, configuration management of systems, identity management” that leads to “business continuity, not just compliance.” The return on investment, as described by the presenters, can be realized much faster if the approach of making Sarbanes-Oxley a sustainable compliance program is taken, rather than a one-time project implementation, and business, and IT leaders work together in the achievement of common goals.

A director at a large financial services company charged with managing the major IT projects for the organization recently hired a small staff to manage the various compliance activities that require participation by the IT organization. She states, “Rather than sitting on the sideline and being a recipient of compliance requests, we have decided to be proactive and run the IT compliance program ourselves.”

She goes on to say that, because of this structural addition to her department, coordination and alignment with overall business objectives are improving and helping IT become more relevant in the organization overall.

While levels of enthusiasm and participation by IT in the compliance efforts vary greatly, there does appear to be a shift toward more compliance ownership and less oversight from traditional compliance leaders (figure 2).

**A LOOK AHEAD**

IT departments appear to be moving in one of two directions in relation to their philosophy of compliance and IT risk management. The first direction (figure 3), and the one that appears to be the most common, is recognition that IT compliance and risk management activities have improved employee behavior, strengthened the overall control environment and raised the prestige of the department. The departments following this direction are taking advantage of the lessons learned over the past decade and moving from a “project” mentality to a sustained compliance function. One IT director of an audit and compliance group at a large software company states, “In an increasingly regulated environment, the ability to demonstrate compliance day in and day out across the company is a requirement for our continued success. If we fail to implement effective controls, there can be significant consequences to corporate performance, reputation and customers. We are moving in a direction to ensure that adherence to IT standards is an everyday activity, not a once-a-year project.”

Her company has created an entire audit and compliance function within the information security organization that not only manages quarterly Sarbanes-Oxley testing efforts, but also has implemented a broad set of audit activities to include all aspects of IT compliance efforts. She further states, “Compliance is a business process that needs to be managed end to end, not just the implementation of tools to manage point-in-time security risks and other compliance risks. Increasing levels of information security risks that jeopardize the integrity, availability and confidentiality of our data will continue to drive the need for strong evidence that controls are being monitored and risks are being managed.”

This philosophy is being recognized by many software companies in today’s market that are moving rapidly to create comprehensive IT risk management platforms to assist with efficient and effective compliance monitoring. Most compliance tools are being designed with the recognition that enterprise-wide IT compliance activities are growing in popularity and senior executives are interested in the monitoring and reporting these tools can provide.

There are companies moving in the other direction (see figure 4). While not that common, some companies are reverting to the “old” IT department, the one that does the
minimum and does not value the positive side effects of the compliance activities to which it has grudgingly attended. These IT departments view compliance activities as a pass/fail exercise, a cost-sink and not part of an overall IT risk management function that adds value to the company. While perfectly within their right to operate in this manner, they are likely missing a great opportunity to transform the IT department of the future.

**CONCLUSION**

Critical to determining which direction IT compliance takes is the leadership within IT and its recognition of the value this function brings to the organization overall. Value beyond the mere act of compliance is beginning to be identified, measured and reported. “IT departments that recognize that IT risk management practices can be implemented as an overarching framework from which a comprehensive IT compliance program operates will be able to achieve more cost-effective and meaningful operations from IT.” The question for each IT organization is what its department will look like 10 years from now.

**ENDNOTES**

1. Pearl, Michael; Personal interview, 10 November 2008
4. Anonymous, Personal interview, 3 February 2009
5. Rogers, Liz; Personal interview, 23 October 2008
6. *Op cit*, Pearl