

Compliance Has Many Faces

John Bace, Lane Leskela, Carol Rozwell

As a result of panel discussions conducted at Gartner Symposia in 2004, compliance management issues are clearer and more-easily explained. The four pieces in this Technology & Society Spotlight examine these issues in greater depth.

ANALYSIS

The Japanese tale "Rashomon" tells the story of four people who witness the same event. Later, when asked to recall what they saw, they tell four completely different stories.

The same could be said about the way some people view compliance.

At Gartner's 2004 Spring and Fall U.S. Symposium/ITxpos, a series of four unique panel discussions provided IT professionals with opportunities to see compliance requirements, procedures and best practices from the perspectives of CIOs, accountants, lawyers, risk management consultants, regulators and vendors. These panels used an academic-style case study of an imaginary company as a starting point. From there, 19 different panelists on four different occasions worked the case (with help from the audience) using an interactive "theater in the round" format. In this Technology & Society Spotlight, we've captured the high-level consensus of these panel discussions in four *Research Notes*.

In simplest terms, what is compliance?

Compliance with any business regulation means interpreting what it says, understanding where your organization currently stands, documenting a plan for achieving compliance, executing it, and devising measures and controls to prove that you've implemented the plan.

For the past several years, corporate compliance in the United States has been synonymous with the U.S. Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act of 2002. The law requires an organization to explain its financial statements — that is, how it got those numbers and why auditors should believe them. For example, firms must now validate their financial numbers against their contracts and transactions.

What is IT's role in compliance?

A sustainable and affordable compliance framework must be underpinned by appropriate IT systems. Many of the necessary IT components (Web-based services, content management, document management, workflow management and desktop integration services) may already be in place, but they must be integrated and standardized across the business.

There must also be a repository that contains details of every process, control and risk. Making such contents available will ensure that everyone knows who owns each element.

IT systems must be able to deliver relevant tasks to the appropriate owners — and by role, if possible. As such, IT has a special responsibility to work closely with finance, internal audit and the CFO to reduce the compliance burden on the organization. This can be achieved by automating manual process controls and, over time, *eliminating* process controls by following a compliance architecture approach to create inherent system controls. Today, for example, in meeting Sarbanes-Oxley compliance, the vast majority of organizational controls involve manual operations. Most organizations have stated objectives to *automate* these controls during the next several years. However, since there's no such thing as off-the-shelf compliance technology, the only way they'll be able to achieve this is by taking available technologies and integrating them to create a compliance infrastructure. The IT function *must* be able to lead the integration effort, because those appointed as chief governance officers or chief compliance officers aren't likely to have IT backgrounds, or even much experience as IT users.

What is the CIO's role in compliance?

CIOs must do more than help business process owners determine their organizations' greatest areas of risk so they can be addressed first. Frequently, CIOs have developed the discipline and

appropriate risk-management methodologies to determine the greatest areas of corporate exposure. With these skills comes the ability to champion the automation of internal controls and contribute significantly to reducing the organization's overall compliance burden. Other corporate stakeholders will tend to want a comprehensive solution involving every IT system, control and process. The CIO must reduce plans to a reasonable scope so the IT organization only has to work on elements that relate directly to compliance requirements — for example, financial systems in the case of Sarbanes-Oxley. CIOs should be prepared to invest large amounts of managerial time to make this happen.

How should IT approach compliance requirements?

Many organizations are spending more than they need to on IT-related compliance work, because they haven't clearly defined the scope of what's necessary and sufficient for disclosure. Some believe that the way to ensure compliance is by duplicating their investments in IT hardware. IT *does* have a role in ensuring that relevant information is available and can't be tampered with. However, the organization also must consider how IT support for compliance activities can be provided on an enterprisewide basis for *all* compliance needs, rather than just implementing "point" solutions for *specific* needs (such as Sarbanes-Oxley attestation).

Instead of reviewing the entire IT infrastructure, including applications and application life cycles, CIOs must create a rational balance between IT work that's essential for compliance and other IT projects that are necessary to support the business.

CIOs must not divert all of their resources to compliance work. They should be preparing to roll out new business applications soon after the initial compliance deadlines have passed. Also, they should involve senior business executives in the allocation of IT resources between compliance work and business projects. Involving senior executives will be easier if there's an enterprisewide governance framework in place for compliance.

In "Answers to Basic Questions About Compliance," six major vendors in the compliance marketplace address the most-common questions that many of their clients have asked.

In "The CIO's Role in Compliance," two CIOs from heavily regulated industries, an accountant, a lawyer and two risk-management consultants explore how IT must be prepared to take a leadership role in achieving successful compliance.

"Best Practices and Survival Tactics for Compliance Activities" looks at what does and doesn't work from the viewpoint of CIOs, an attorney, a former regulator, an accountant and a risk management consultant.

Finally, "Compliance Management Solutions Can Create Improved Business Performance" reports on how attitudes toward compliance are changing, and explains why more senior managers are paying greater attention to compliance (it has a greater effect on all aspects of business operations).

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509