

Reducing Compliance Friction Points

By Gregory Toto, Vice President of Product Management, BigFix Inc

Increasing requirements for organizations to comply with international, national and local laws and regulations is creating new sources of friction for Information Technology (IT) organizations. Friction here is defined as a force that slows progress to higher level goals, requires energy to overcome, and often generates considerable heat. Certainly, every reputable organization desires to operate in accordance with laws and ethical standards. The issue here is that recent trends in international and national laws have escalated demands on IT organizations to maintain and report information on organizational legal compliance.

IT organizations get involved with compliance in two ways. First, IT infrastructures contain repositories of information about overall business practices and operations that are subject to legal standards and regulations. Second, IT practices and assets may themselves be the subject of compliance requirements in such areas as data privacy, security of on-line business transactions, etc. Either way, the new wave of compliance requirements forces IT organizations to devote more resources to reporting on compliance status and addressing and remediating areas of non-compliance.

While these activities are essential to the ability of an organization to transact business, many managers view compliance as diverting resources away from IT's traditional mission of helping organizations run more efficiently, lower business costs, serve customers better, and create new business growth opportunities. This can make legal and business compliance issues a source of friction for an IT organization, both in terms of adding to the overall workload and creating opportunities for conflict with non-IT managers, regulators and other constituencies.

For this reason, organizations need to find ways to, at minimum, reduce compliance frictions, or better yet, convert IT workload devoted to compliance into activity that helps organizations achieve broader goals. Based on experience working customers in the US and Europe, I can recommend four ways to reduce compliance friction.

Focus on Compliance "Customers"

First, since organizational compliance efforts may involve different divisions within an organization that may have differing or even overlapping compliance agendas, IT organizations must first recognize that there may be a number of different internal "customers" for compliance information. The finance department, for example, may be concerned with compliance with accounting and financial market regulations. Legal staff may focus on business records retention, contracts, and anti-monopoly law. The human resources department will look to IT for information on employment conditions or medical/health insurance data. Even the IT department faces its own compliance requirements when it comes to software license usage tracking, meeting internal service level agreements (SLA), or achieving best practices certifications.

The advice here is that IT organizations should take a customer-focused approach to compliance programs. This means IT needs to understand the needs of each compliance "customer" and work with them to determine what kinds of compliance services they need and how to provide them. This can evolve into an SLA-based approach to providing IT support for achieving various compliance agendas around an organization.

Real-Time Visibility

Second, as reporting is often the central role of IT in compliance, it is critical that IT have a complete and up-to-minute visibility into all information relevant to an organization's compliance status. Reporting that relies on fixed-point-in-time assessments that take place annually, monthly, weekly, or even daily can overlook activities that may be significant to a compliance program. For example, any delays in detecting and repairing vulnerabilities can leave an organization at risk to attacks and intrusions that take advantage of a particular vulnerability. This is particularly true at a time when hackers have developed a proven ability to exploit security vulnerabilities almost as soon as computer companies and industry bodies warn users of their existence. Under these circumstances, waiting a week or a month to learn whether an organization complies with the latest standards for system security configuration is simply not acceptable.

Fixed-point-in-time scanning technologies are also finding it hard to cope with organizations that manage significant proportions of mobile workers or computer assets. Assets that are not logged on to an enterprise's network at the time of a scan, do not appear in reports and are beyond the reach of administrators for purposes of fixing problems.

Technologies that provide real-time reporting, however, are currently on the market in the form of client agent-based solutions that continually report on asset configuration status, whether hard connected to an enterprise LAN or more loosely linked in via the Internet.

Self-Service Reporting

Third, the more an IT organization can automate the process of compliance reporting and make compliance information available to internal customers without intervention from IT staff, the better. The ideal situation here is for internal compliance customer to have instant access to up-to-date, preformatted reports designed to meet their specifications. This can reduce IT staff workload by reducing the need for them to spend time to "running a report" for a non-IT manager.

Self-service reporting at this level requires understanding reporting requirements in advance as enabled through the customer focused "compliance SLA" approach mentioned earlier; non-stop, automatic data reporting; automated processing of data into reporting formats; and making compliance reports accessible to qualified compliance customers on line. Self-service reporting reduces IT staff workload, improves the quality and currency of information available to compliance customers, and increases compliance customer satisfaction by reducing effort required to access information they need,

Integrating Reporting and Remediation

Fourth, there is no reason that compliance reporting should be treated as a separate function with no relationship to IT operations or security management. The ideal here would be to use tools and processes that combine compliance reporting with security IT asset configuration management. By creating a single infrastructure for compliance reporting and asset management, the IT department can reduce its workload and move the organization towards a compliance posture that enables them to find and fix compliance issues before they become serious problems that expose an organization to legal, commercial or social consequences.

From Compliance Attainment to a Virtuous Cycle of Governance

IT managers should remember that compliance is really a governance issue that involves an entire organization, not just the IT department. The trend of new laws and regulations certainly makes IT an important component in maintaining organizational compliance, but IT plays a supporting rather than a leading role. A complete compliance program will bring together all groups within an organization with compliance responsibilities.

Ultimately, the goal of any compliance program is not merely to “get by” relevant legal and business standards but to align compliance efforts with overall best-practices management of IT assets and processes. Here, an organization that can pro-actively manage compliance programs at a high level of organizational maturity will probably also be able to manage its overall IT programs at an equally high degree of operational efficiency. In this way, reducing compliance friction becomes an important means of developing IT into a well-oiled value-generating machine.
