

The Path to Continuous Compliance Management

Ted Ritter, Research Analyst

Executive Summary

As the role of the CSO shifts from technical security expert to risk mediator, manager and advisor, compliance is rapidly becoming the domain of the CSO. In this role, the CSO is faced with the continual tug-of-war in the corporation between legal, business and IT. To make matters worse, the CSO – as Chief Risk Officer – is put in the position of keeping the company out of trouble, without having any control over the direction or the company, or the actions of IT, business and legal. The only way that the CSO can affect risk and manage risk is through implementation of a strong compliance management process. Compliance management is the heart of governance and risk management and as such, it's the main tool in the CSO tool box.

Compliance is a complex issue and it requires a unique combination of technical, legal, business and management skills. Compliance itself requires solving the equivalent of a multi-variable equation: regulations, control frameworks and change. To achieve continuous compliance management, CSOs must implement tools and processes that automate and streamline the compliance management process. The first step is implementation of logging, eventually culminating in the establishment of a continuous compliance management solution that not only reports on what has happened, but implements triggers, monitors and controls to prevent what is going to happen.

The Issue: The Evolving Role of the CSO - From Security Technologist To Risk Mediator

The Chief Security Office (CSO) position is fairly new, having first emerged in larger corporations in the late 1990s. Today, it's a standard role in most organizations of even medium size. The CSO's role varies, but typically it involves leading IT's security efforts, security policy development, and security technology investments. Increasingly, though, companies are recognizing that the CSO's central and fundamental job goes well beyond security to evaluating the risk of different business choices and then directing the appropriate mitigation strategy.

In many cases, coming up to speed in these areas is forcing security professionals to broaden their insight into non-technical fields. In particular, they must translate laws and regulations into technical requirements. The reality for the CSO is that their role is evolving from one of a technical security expert to one of a risk advisor, mediator, and manager.

Being a CSO in a public or regulated organization is like standing in the middle of a three-way tug-of-war, between legal, IT and business departments, driven by legal and regulatory pressures, such as: SOX, HIPAA, GLBA, CA SB1386, FERPA and FRCP.

Fundamentally, the CSO is beholden to IT – the traditional CSO role - to support the continual march of IT upgrades and enhancements. In this role, the CSO is under constant pressure to assess the risks of new technology. To illuminate this point, Nemertes research shows that two-thirds of organizations in the *Security and Information Protection* benchmark have avoided a new technology due to security concerns. This pressure on the CSO, from IT, is ratcheting-up a notch as the IT shop moves toward emerging technologies, including: services-oriented architectures (SOA), virtualization and unified communications and collaboration (UCC).

Meanwhile, the CSO is sometimes seen as “sales prevention” by the business side of the house. The business is continually pushing to be more agile, flexible and competitive; to do things better, faster and cheaper. In other words, pressure to move faster, with less overhead, and in a more integrated/coordinated manner with trading partners and customers: all factors that complicate the CSO's job.

Finally, the CSO role is closely coupled to the legal side of the house. Traditionally, Legal has been the home of compliance, but as compliance moves from a financial and accounting function to an IT-centric function, the CSO is becoming the lightning rod for legal departments that need to exert pressure on the organization without the technical authority and knowledge to affect IT. Reflecting this growing linkage between CSO and Legal, 16.7% of companies participating in *Security and Information Protection* have CSOs reporting to the CEO or CFO rather than to the CIO.

The Realities – and Cost – of Compliance

The reality of security and compliance is that the implementation, monitoring and reporting are rapidly becoming the responsibility of the CSO: 20.5% of participants in *Security and Information Protection* identified this as a security priority in 2007, rising to 30% in 2008. Further, compliance is already a core, CSO team function for 81.5% of participants. A good confirmation of this relates to metrics for success. One of the two most frequently cited metrics for success in security is, in essence, that the CIO not be front-page news. No organization wants to be the next TJX or California Pension Board. With public disclosure of security breaches mandated by laws like California SB1386, compliance is the hidden driver behind the metric and so behind much of what IT pursues in the name of security.

There are real costs for compliance (OpEx and CapEx), and even greater potential costs (tangible and intangible) for non-compliance: credibility, legal action, regulatory action, market action, etc. When asked how much they spend on compliance, most participants say they don't know, since there isn't a separate budget under which such things are tracked. Most are sure it isn't small change. "A nice little bundle," as the security architect at a transportation company puts it; "an absurd amount," says the security manager at a bank. IT executives, however, certainly are sure of the parts of the regulatory landscape that are costing them the most. Despite not having exact figures, it is clear to organizations which regulations are the most costly to comply with. Somewhat surprisingly, despite the volume and intensity of griping about it, SOX is not the most onerous regulation, according to participants. That honor goes to the various vertical-specific federal regulations such as the Health Information Portability and Accountability Act (HIPAA) or the Graham-Leach-Bliley Act (GLBA) (Please see Figure 1: Cost of Compliance, by Regulation, page 4).

One cost that is straight-forward to track is OpEx costs. Participants in *Security and Information Protection* have a median of 3.25 and a mean of 4.8 FTEs devoted to compliance activities within their IT security organizations. Much of the work of compliance staff in IT comes down to two things: auditing and reporting, on the one hand, and managing archiving and recovery on the other. Despite extensive hype in the marketplace, IT still uses human eyes to review, and human hands to generate, compliance reports on security logging data. These are obviously not the best uses of time for security staff, since much of the work can be automated, and so these are fertile areas of development. The challenge is that automation without organization is fruitless. Organization comes from sorting out the relationship between governance, risk and compliance.

Top Regulations by Cost-to-Comply

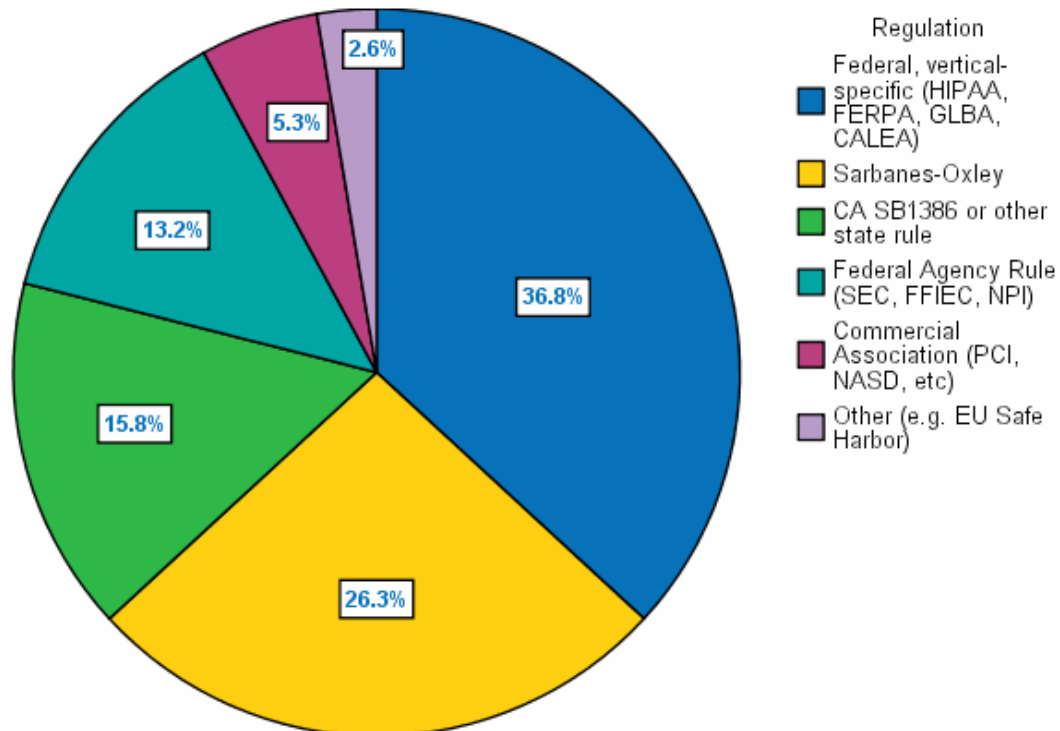


Figure 1: Cost of Compliance, by Regulation

Sorting Through Governance, Risk and Compliance - It all Comes Down to Compliance!

The CSO, standing in the cross-fire of IT, legal and business, is in a difficult position. Essentially, the CSO is tasked with keeping the ship afloat without any direct control over the rudder and throttle! In other words, the CSO doesn't set the corporate goals and doesn't manage sales, production, or IT, yet he/she must make decisions that keep the organization operating within the acceptable level of risk. The way that the CSO accomplishes this is by driving compliance; as the foundation of good corporate governance and risk management.

At a high level, governance refers to the set of processes that keeps the organization alive and healthy: establishing the right course; adjusting to obstacles along the way; avoiding trouble; and doing all of this in a transparent and timely manner. Risk management (as defined by the ISO) is the "systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating and controlling risk." Finally, compliance is the establishment, enforcement and monitoring of controls (technical, operational, management and compensating) that verify and validate that internal (corporate

policy) and external (government and industry regulations) requirements are being met.

In the nautical example, governance is based on the ship's manifest, navigation rules, maritime law, and the ship owner's policies; risk management is using the nautical charts and weather charts to assess the relative level of risk that must be assumed to stay on the course charted by the captain; and, compliance is having and monitoring depth gauges that alert on approaching shoals and navigational equipment that alert when the ship is off-course.

For the Sea-S-O, the situation may be: the bow clears 20 feet, the depth chart says 30 feet, there are 10 foot swells predicted and the depth gauge is only accurate to 3 feet. For the CSO, the situation may be: IT is deploying SOA, countless new interfaces will be exposed, and the network has no XML or web services security. In both cases, the result is a level of risk that can only be monitored, managed and reported through compliance. The bottom-line for both the Sea-S-O and the CSO is that without compliance, there is no governance or risk management. Just as the Sea-S-O cannot assess risk without a working depth gauge, the CSO cannot assess risk without a working audit log. Likewise, it doesn't matter how well, or poorly planned the course; if the GPS system is down and the crew doesn't know how to use a sextant, the ship is in trouble!

Compliance Management Dynamics

Compliance is a complex process that may be broken down into three components (Please see Figure 2: Compliance Management Dynamics, page 6):

1. **Regulations.** Regulatory mandates drive compliance. All organizations are susceptible to multiple regulations, with overlapping requirements. For example, regulations such as HIPAA, PCI and FERPA all have privacy mandates that tie to personally identifiable information (PII): medical records, credit card numbers and student account info, respectively. At the same time, geographic differences impose added complexity to sorting out the regulations. Some countries have shared regulatory frameworks – EU Countries, for example – while other countries impose opposing regulations. For example, one country's privacy laws may be in conflict with another country's disclosure and eavesdropping laws. This is an area where CSO's must consider the geographical distributed nature of the company and the associated laws, regulations, customs and best practices.
2. **Control Frameworks.** The second component consists of the control frameworks that must be put in place to achieve compliance. There are security practice frameworks and guidelines, including the Control Objectives for Information and related Technology (COBIT), ISO27001 (formerly, ISO17799) and the NIST 800-Series. Use of these frameworks is growing rapidly—nearly all participants responding on this point in *Security and Information Protection* are at least looking at ISO 27001 or COBIT, even if they aren't formally adopting them. Just as there is overlap in regulations, there is overlap in control frameworks. For example, most identity/privacy related regulations require strong audit, identity and access controls; and,

financial oriented regulations require some level of archive and separation of duties controls.

3. Change. As organizations grapple with regulations and control frameworks, IT shops are always in motion and regulations are always changing. The CSO must track the controls necessary to achieve compliance with the myriad of regulations, and continually assess how changes in the underlying IT organization may affect existing and planned controls. This is particularly true as organizations shift IT development from applications to services. For example, a service that is not properly retired places the organization at risk due to the chance that the service remains active, without being continually monitored for compliance with current requirements, let alone vulnerabilities, or exploit.

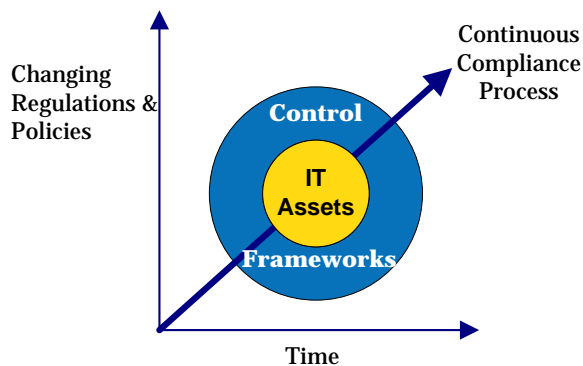


Figure 2: Compliance Management Dynamics

To keep the corporate ship on course and off the shoal, the CSO must implement a compliance solution that is able to support these compliance management dynamics. The ultimate goal is to achieve a continuous compliance solution that supports these requirements in an automated and proactive manner. There are two aspects that the CSO must consider: process and tools. The processes associated with the support of the compliance management dynamics is discussed in an upcoming Nemertes Issue Paper. The tools associated with continuous compliance are discussed below.

Going from Framework to Real Work – The Road to Continuous Compliance Management

Most organizations are on an evolutionary track to continuous compliance management, starting with of event logging. After all, if one doesn't have sufficient audit trails in the form of logs of network, system and application activities, it is impossible to demonstrate compliance. Approximately 90% of participants in *Security and Information Protection*—whether they aggregate logs or not—do some kind of log monitoring, either

manually or with a logging tool. However, at least a quarter of these participants do so only during business hours (9 to 5) though, or even less frequently.

The next step toward continuous compliance is log aggregation. Approximately, 64% of participants in *Security and Information Protection* collect logs from many sources and aggregate them for analysis and retention. Just under half of that group aggregate all infrastructure-related logs—server, router, firewall—and some even collect desktop logs as well.

Once logs are aggregated, the next step is real-time analysis and response. About half of participants in *Security and Information Protection* are doing some kind of real-time analysis and response to logged events, running all the time. This is mostly via managed IDS/IPS tools or via alerts or alarms generated within the system logging the event in the first place.

As discussed above, log management and monitoring still involves a lot of costly manual intervention. Organizations are looking to take compliance management to the next level by implementing automated systems that are designed to streamline and focus the compliance management process. About a quarter of participants in *Security and Information Protection* are using dedicated log management systems or a full-blown Security Information Event Management (SIEM) tool, and another quarter are either developing or evaluating one.

Though not initially developed as compliance solutions, most SIEM tools are moving in the compliance management direction. Right now, it appears that the SIEM tool is well-positioned, since it is focused on the security health of all the key components of the IT organization: all components that affect compliance. However, there is a caution here, since participants in *Security and Information Protection* are also finding implementing a SIEM to be tricky. CSOs looking to achieve compliance management via SIEM tools need to take a step back and make sure that the SIEM tool they are using – or choosing – is really the best tool for compliance management. For example, does the SIEM tool support the establishment, implementation and tracking of the IT controls necessary, to meet the regulations, required, and support the continual movement of the IT and business requirements? If the answer is “yes” then continue on course. If the answer is “no” then it’s time to slow-up and re-plot a course that will get the organization on track for continuous compliance management.

Recommendations

The CSO is clearly in the hot seat for implementation of a continuous compliance management solution. As discussed in this issue paper, the CSO must map the regulations, frameworks and change dynamics to plot a compliance management course (process and procedure) and then implement the tools necessary to stay on course. Together, tools and process come together to achieve continuous compliance management that successfully manages the organizations compliance efforts - keeping the ship off the shoal – while balancing the pressures applied on the CSO by the legal, IT and business sides of the organization.

About Nemertes Research: Founded in 2002, Nemertes Research specializes in analyzing the business value of emerging technologies for IT executives, vendors, and venture capitalists. Recent and upcoming research includes Web services, security, IP telephony, collaboration technologies, and bandwidth optimization. For more information about the analyst, please contact Nemertes at research@nemertes.com.