

## QUESTION &amp; ANSWER

## CSO INTERVIEW: Regulatory pain is a two-way street

By Bill Brenner, News Writer

**Y**ou might not expect someone from the agency enforcing the Sarbanes-Oxley Act to describe regulatory compliance as something bogged down with “bureaucratic overlap” that’s “killing” enterprises. But that’s exactly how Chrisan Herrod sees it.

As CSO of the Securities and Exchange Commission [SEC], she is responsible for making sure the agency meets many of the same standards it enforces on others. Like many security/compliance professionals, she has her own war stories to tell.

One example — a recent Government Accountability Office [GAO] report that took the SEC to task for not implementing “effective electronic access controls” like “user accounts and passwords, access rights and permissions, network security or audit and monitoring of security-relevant events...”

In this Q&A, Herrod explains why organizations like GAO must look at compliance as more than the machinery a company puts in place. She also explains how the private and public sectors can work together to bring sanity to the process.

**Since the SEC is a regulatory enforcement agency, it must be difficult when another agency scrutinizes your own compliance controls.**

Herrod: When people give us feedback on the difficulties they’re having, I understand. We go through it, too. The GAO’s last audit of the SEC is a good example. They published a scathing report citing the SEC’s lack of material controls. But they could never prove there was ever any financial control problem stemming from a lack of information security controls.

Our control mechanisms are very secure. But we were criticized for not having specific [technological] controls in place. In my view, it’s all about looking across the spectrum, looking at all

your controls, not just the technological aspect. It’s about your physical control, your personnel control, where you store paper — all those kinds of things. If you have sound controls and sound recordkeeping, you’re taking reasonable steps to comply even if a technological control hasn’t been implemented.

**The GAO said the SEC hadn’t implemented “effective electronic access controls.” What did they mean?**

Herrod: We were using a manual, paper-driven access control process. Since the GAO report was published, that’s being replaced by an automated identity management system which will link all of our access controls at the system and application levels so we can manage SEC employee and contractor access from a single workstation. Additionally, we purchased a central monitoring system, ArcSight, which will integrate the monitoring of all our perimeter defense and application level tools into a single monitoring capability.

**Talk about the SEC’s overall security posture and how it falls within the zone of reason you referred to.**

Herrod: The SEC uses a combination of technology, process and management controls to ensure that we are in compliance with the Federal Information Security Management Act [FISMA]... We implemented both process and management review controls with respect to our certification and accreditation program, our training and awareness program and our incident response programs. We have a very good track record with respect to our perimeter security and defense in-depth strategy. We’re working to improve our internal technology controls, which is at the heart of [the GAO findings].

“  
**Additionally, we purchased a central monitoring system, ArcSight, which will integrate the monitoring of all our perimeter defense and application level tools into a single monitoring capability.**

Chrisan Herrod  
Chief Security Officer, Securities and Exchange Commission

”  
**Compliance officers often complain of overlap in the regulations they’re responsible for, as well as the time and money they waste sorting it out. What’s your view?**

Herrod: They’re right. There’s so much bureaucratic overlap right now that it’s sinking us. We need a common baseline of standards. There has to be a convergence between the public and private sectors.

**Do you think there needs to be a law that fuses together the common requirements of Sarbanes-Oxley [SOX], HIPAA, Gramm-Leach-Bliley [GLB] and others?**

Herrod: I don’t think we should expect one overarching set of regulatory guidelines. But I think there could be a more centralized, simplified auditing approach. Instead of forcing people

to work off several different auditing reports for several different regulations, there could be one auditing report that accounts for the common requirements and works for everyone. I think that can happen.

**Whose responsibility is it to make that happen — the private sector or government?**

Herrod: The easiest, best solution would be for Tom Davis' committee to take a hard look at these regulations, especially those for publicly-traded companies that are already heavily regulated. [Editor's note: U.S. Rep. Tom Davis is a Republican who represents Virginia's 11th Congressional district and chairs the House Committee on Government Reform.]

The tea leaves are saying that SOX will be expanded to affect more and more entities. Davis' committee has the power to streamline the process but it hasn't happened yet. I think it would be simple enough to do. One thing we could do is get all the auditors together to hammer out the common criteria they look for. It's crazy to have to respond in multiple ways with multiple reports. The government and auditing industry could get together to work on this. They should, because the overhead is killing us.

**What kind of companies are shouldering the most overhead?**

Herrod: The Washington Post Company is a good example. In addition to the newspaper and other media properties, it owns colleges [through one of its subsidiaries, Kaplan Inc.]. The company is responsible for so many regulations. Universities are in the same situation. Many [companies] are publicly traded and are

bound by both SOX and HIPAA. As companies grow and diversify, they don't look at regulations as part of the acquisition/merger equation. But it becomes a big issue. They're not thinking about the regulatory impact, but they have to start because it's a huge overhead issue.

Industry has to get very vocal about the overhead they're sustaining to meet these different regulations. They have to start with their congressmen and make it clear to them how big a burden it's becoming. Private industry also has to be part of the solution. It has to make suggestions on how to streamline the process.

**Where can compliance officers find a set of guidelines that capture the crux of the different regulations they're dealing with? One example we've heard before is the Federal Trade Commission [FTC] Safeguard rule.**

Herrod: The FTC has done a very good job developing solid guidelines around information security management and technology controls. My understanding is that they based it on ISO 17799, a security standard developed by a number of countries. The guidelines really capture the requirements you're responsible for whether you're under SOX, GLB or HIPAA. ISO 17799 was developed by information security professionals, not auditors. One of the things I like about it is that it groups things into technological controls, management controls, process controls. It pays homage to the fact that information security is about more than technology.

**What has the SEC been doing to help the private sector get its arms around the regulatory soup?**

Herrod: The SEC solicited feedback this year from companies that have gone through SOX compliance and have been audited, specifically on section 404-403 — the part that deals with information technology controls around financial systems. We asked companies and auditors what the major pain points were. One of the major pain points was the lack of clarity on what standard would be good to follow. They were basically saying the government isn't telling them what the minimum requirements are for them. There are still big gaps. There hasn't yet been a policy offering that clarity from the SEC or PCAOB [Public Company Accounting Oversight Board], which oversees the auditing industry. But the feedback is loud and clear. I can certainly validate from the conferences I've attended that everyone is asking: What minimum standard are we being held to?

**The SEC recently issued a statement saying the cost of meeting Section 404 of SOX is out of control and that auditors are making overly broad interpretations of what companies need to do. When was that conclusion reached?**

Herrod: That came out of hearings the government had. In the end, the government isn't going to be overly descriptive. The regulations will tell you what needs to be done but they won't go into greater detail about how you need to do it. And Auditing firms will always take a more conservative look at what a company has to do. We felt it was important to make the point that you need to take steps that are within reason based on how big you are, what you do and what your budget is.



[About ArcSight](#)

ArcSight, the recognized leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM™ enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading global companies across all verticals—and more than 20 of the top 30 U.S. federal agencies.

[For More Information](#)

To find out how ArcSight can help you with your enterprise security management needs, contact ArcSight at [info@arcsight.com](mailto:info@arcsight.com), call (408) 864 2600 or visit us online at [www.arcsight.com](http://www.arcsight.com).