


[IT Jobs](#) | [Downloads](#) | [Columns](#) | [Subscriptions](#) | [Search](#)
[Australia's Magazine for Information Executives](#)
[CSO Online](#) | [CIO Government](#) | [CIO Connected](#) | [CIO Conferen](#)
[CSO The Resource for Data Security Executives](#)

Friday, 17th December 2004

The Sarbox Conspiracy

CHRISTOPHER KOCH, CIO

12/07/2004 12:13:08

Sarbanes-Oxley compliance efforts are eating up CIO time and budgets. Worse, CIOs are being relegated to a purely tactical role. And that may be the CFO's plan.

When CIOs began installing ERP systems in the 80s and 90s, they unwittingly took something that used to belong to CFOs: financial controls. The things that accountants used to monitor manually — such as making sure that two signatures from the right people went on every cheque, or reconciling purchase orders against invoices — all became automated inside ERP systems. The meticulous audit trail that controllers and accountants had established over generations for demonstrating that money was being handled properly (think of black, leather-bound ledgers and long ribbons of adding machine paper) disappeared into those ERP systems without a trace — or at least without being properly documented, and certainly not to the extent now required by the 2002 Sarbanes-Oxley Act, aka Sarbox.

Today, CFOs want those controls back. If they don't get them, they believe they could go to jail. Section 404 of the Sarbanes-Oxley Act mandates that CFOs have to do more than simply pledge that the company's finances are correct; they have to vouch for the processes used to add up the numbers (see "What Section 404 Says", page 67).

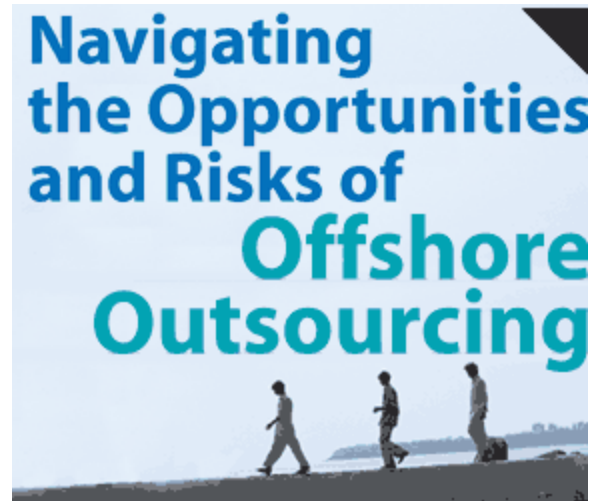
Sane people don't want to go to prison. They can even get a little frantic about it.

That's why CIOs perhaps can forgive their CFOs for getting aggressive when it comes to taking control of Sarbanes-Oxley compliance efforts. What CIOs shouldn't forgive, or take lying down are their CFOs' attempts to freeze them out of the process.

A recent survey by research company Hackett Group found that just 12 of 22 companies surveyed had IT representation on their Sarbox steering committees. Among 75 public companies that Gartner surveyed at the end of last year, just 63 percent said IT was involved

Partly, this may be because many companies have been slow in getting their Sarbanes-Oxley efforts up and running. Only 65 percent of Gartner's respondents even had a Sarbox steering committee. Twenty-eight percent had no plans to form one.

But some CIOs see a darker agenda at work — a conspiracy. They fear Sarbox has become a stalking-horse that CFOs are using to assert control over IT and displace the CIO as the



company's business process expert. Egging CFOs on, this theory goes, are the Big Four accounting firms, desperate to reassert themselves after the Enron debacle (which turned the Big Five into the Big Four after Arthur Andersen bit the dust) and needing consulting revenue to replace what they lost when most split off their consulting divisions.

"Finance and accounting organizations have been pushed to the background recently as IT and supply chain have been driving where companies are going," says one disgruntled CIO who declined to be identified. "Sarbanes-Oxley is the revenge of the bean counters. It's a wedge for the accounting profession to get control of the business again."

"CIOs are getting left out of Sarbanes-Oxley efforts, and it's a travesty," says Garry Lowenthal, CFO of Viper Motorcycle and chairman of the Finance and Technology Committee of Financial Executives International (FEI), an association of senior financial executives. (Lowenthal is sufficiently concerned that he is helping to set up a joint session between FEI and the Society for Information Management [SIM] at SIM's annual meeting this September to talk about how IT and finance can work together on Sarbox.)

"I'm hearing stories about CFOs not including CIOs in their compliance visions," Gartner research director Rich Mogull says. "I think that's a big mistake."

The Dark Agenda

Right now, CFOs are setting up compliance committees, often headed by their controllers and staffed by internal auditors and consultants from the Big Four accounting houses, and sending them out in pursuit of any and all business processes and IT systems that could have any impact on the balance sheet. IT systems across the country are glowing eyeshade green as accountants flock around them to figure out how they work and document those buried controls.

For CIOs, this can be a huge distraction and an enormous energy drain.

"We've taken a substantial productivity hit from this," says Brunson White, CIO of utility company Energen. "We didn't do much besides governance work last January. Sarbanes has pulled some of our best resources and altered our plans for other projects."

Sarbox is also expensive. Another utility CIO, Dennis Klinger of Florida Power & Light, says his company has already spent "multiple millions of dollars" on compliance, most of it on labour. And just as companies are starting to loosen their purse strings, much of that money is coming out of IT's hide.

But where there's pain, there's also opportunity.

If CIOs can take Sarbox beyond mere compliance, and automate and streamline business processes and financial controls so that the cost of compliance goes down over time while business performance improves, they could become heroes. But if they just play a tactical role focusing only on IT-specific controls and leaving the rest to the CFOs and the accountants, they could fix a hard, clear varnish over the view in many executive suites that IT should be forever subservient to finance.

Which, according to many, is just what finance has in mind. As a former corporate vice president of IT, C Lee Jones, chairman and CEO of Essential Group, a pharmaceutical services company, has had front-line experience on both sides of the IT-finance battleground, and he says that many CFOs would like to see CIOs left out of the Sarbox equation. Why? Because, he says, "it would give CFOs control over one of the largest fixed costs in the company: IT".

It's beginning to look as if Sarbanes-Oxley will be the greatest test yet of CIOs' standing with the enterprise.

The Sarbox Disconnect

Running Sarbanes-Oxley efforts is not an option for most CIOs. Sarbox is about financial processes. And each year when they sign off on the numbers, it's the CFOs' necks on the line (along with the CEOs'). "Controls and processes around financial reporting indicate the money guy should be intimately involved [in Sarbox]," says AMR vice president of research John Hagerty. A recent AMR survey found that 72 percent of Sarbanes-Oxley compliance teams were led by finance, and just 4 percent by IT. (The remainder were led by other business functions plus legal and the board of directors.) But CFOs will not be able to prove compliance without the CIO. In most cases, the CFO's expertise ends where his numbers feed into information systems.

Most CFOs are aware of that, of course. However, they have options about where to go to get help. They could delegate compliance to internal audit (another group lacking a good understanding of IT issues) or hire external consultants. But if CFOs do an end run around IT and keep Sarbox efforts within the domain of the accountants and consultants, they could lose an opportunity to make the business run better. Hackett Group found that 47 percent of companies it recently surveyed still use stand-alone spreadsheets as part of their financial reporting process, meaning that the controls used to trace and audit the processes are essentially manual. Somebody throws numbers into a spreadsheet and passes them to someone else until they wind up in the annual report. Manual financial controls, as any auditor will tell you, are time-consuming, labour-intensive and costly; they're why companies abandoned those black ledgers in the first place.

"If you can automate it, and make it repeatable, you can know the controls," says Marc West, CIO of video game maker Electronic Arts. "If it's manual, it's more difficult to confirm the process and test it."

AMR estimates that of the roughly \$US3 billion spent on Sarbanes-Oxley compliance in 2003, about 90 percent was spent on internal staff and consultants. To keep Sarbox from becoming an annual, recurring nightmare, companies need to automate financial controls (documenting them this time) and replace some of the labour-intensive manual detective work with software and hardware. That shift needs a leader. And that leader logically should be the CIO because the CIO will have to maintain and support those automated controls.

But just like Y2K, consultants and vendors are descending upon CEOs and CFOs and selling them magic-bullet software solutions for Sarbanes-Oxley over the heads of CIOs. It's ERP all over again. The financial controls gap inside most ERP systems today is partly the product of the communication gap between those who bought ERP systems (CEOs and CFOs) and those who installed and maintained them (CIOs). ERP projects went sour when business leaders and CIOs could not agree on how best to automate business processes in ways that could be integrated, supported and maintained by IT. Sarbanes-Oxley could easily lead to that same disconnect.

Sarbanes-Oxley means CIOs and CFOs need each other more than ever. Whether they will ever get around to admitting it is another matter. But if someone needs to swallow his or her pride and make the first move, it's the CIO.

The CIO's Dilemma

Today's corporate climate is not, however, conducive to compromise. Consultants and internal auditors are getting in CIOs' faces and demanding tighter controls in IT without deep

knowledge of either Sarbanes-Oxley or IT.

"I've been told that I now need to submit every requisition to finance for approval before I can spend my budget," says one angry manufacturing company CIO who declined to be identified. "The CFO has delegated it to the controller, who has hired all these young auditors and consultants who think they're on a mission. They see Sarbanes-Oxley being above and beyond everything else we're doing. It's annoying because there are more important things we should be doing." Even though she is part of the company's Sarbox steering committee, this CIO has given up hope that the project will lead to the kind of process improvement and automation that could provide a long-term benefit to the business. "Everybody will do what they have to do to get through the compliance door, and the funding and overall attention and priority for the other process improvements will go where they always go — to the bottom of the list," she says.

Mostly, CIOs resent Sarbanes-Oxley. IT has been suffering through a funding drought since 2000, and now that corporate revenue is finally bubbling up again, Sarbox has cut to the front of the line. "We haven't been able to get much funded," says Electronic Arts' West. "Now here comes Sarbanes-Oxley and you have to find money in your budget to document processes. It's frustrating."

West is trying to turn that frustration around by using Sarbox as a lever to revamp governance processes across the business and in IT. "I think this will be one of the best things for IT in the long run because it's an opportunity to improve the ways we do things," adds Brad Friedman, vice president of IS for Burlington Coat Factory and the Sarbox point man for Burlington CIO Mike Prince. "You have to brainwash yourself into looking at it like that or you will dread it, because it's not a one-time event."

But Friedman acknowledges that he's having a hard time knowing where to start. Like many IT executives, he is desperately seeking guidance for this brave new world of Sarbox-enabled governance.

"If you read through the control objectives in Sarbanes-Oxley, they're very general," says Friedman. "Trying to burrow down to the detail and understand what will be looked for by the external auditor is very difficult. It's also difficult to draw the line between IT processes, operational processes and financial processes."

The CIO Solution

At utility NStar, CIO Gene Zimon took an early leadership role by suggesting that the company approach Sarbox the same way it did Y2K. Accordingly, NStar created an overall steering committee that meets monthly and includes the top functional executives from around the company. Zimon volunteered his program office director to help coordinate the effort. Working with the finance group and consultants, the project leadership parsed the project into 10 major processes by reverse engineering the balance sheet and income statement preparation process. "We took the numbers and worked backwards to find every system that contributed something to each of them," says Zimon. Each of the 10 processes was treated as a distinct project, each with its own steering committee, a business sponsor, internal audit consultant, and a business and IT lead assigned to do the dirty work of ferreting out the controls, documenting them and resolving any gaps in the process. "The most important thing was defining the areas we wanted to look at, to make it all real and measurable," Zimon says. "Otherwise, it all seems too vague."

At Energen, CIO White is taking the same reverse engineering approach to controls, trying to automate the ones he can. One is change management for Energen's ERP system. Right now,

the process for making a change to the system — say a tax rate change or a bug fix — is “arduous and requires many sign-offs”, says White. Any changes that can affect financial data will have to be reported under Sarbanes-Oxley, and if, for example, a bug in the ERP software means past financial data was not correct, the company may need to restate earnings. That means change management must be much more carefully documented and monitored than in the past. So White is planning to automate the change request and sign-off processes to speed things up as much as possible. But he’s still worried that the new levels of scrutiny — and the coming requirement in Sarbanes-Oxley Section 309 that material changes to financial be reported in real time — will prevent those changes from happening as fast as some in finance would like. “There isn’t a whole lot more time to milk out of the change process,” he says. “If it takes a week then that’s the way it is. But people are already telling me it’s not fast enough.”

The Knowledge Gap

Without a good playbook for Sarbanes-Oxley, IT and business executives find themselves dependent for advice upon external auditors and consultants. But according to the CIOs and analysts we spoke to, consultants are also trying to figure out what compliance means. And that’s yet another sore point for CIOs.

“I’m not getting any good advice about what I’m supposed to be doing from the consultants or the external auditors,” says the anonymous manufacturing CIO. “They have no clue what Sarbox means for IT yet.” Adds Gartner’s Mogull, “The most common complaint I’m hearing about the auditors is they aren’t providing enough clear guidance.” When he challenged some of the auditing firms with this, their response was that the rules haven’t yet been finalized by the US Securities and Exchange Commission. “I said, Well that’s fine,” recalls Mogull, “but who are you taking people’s money then?”

Complicating the situation is the long-time split that has existed between financial auditing and IT auditing inside consulting firms and the Big Four accounting firms. Financial auditors have traditionally focused on controls and overall business governance, while IT auditors have consulted with CIOs on best practices for running IT. And just like the businesses they serve, it’s financial auditors, not the IT auditors, who are running Sarbox consulting engagements. This can lead to IT issues being ignored or shoved to the backburner. “They send in financial auditors and IT auditors but they are usually two separate teams that haven’t created a [joint strategy,” says Sharon O’Bryan, founder and president of consultancy OAS and a former Big Four IT auditor. This is yet another reason why IT may be left out of strategic planning for Sarbanes-Oxley.

With so much potential for confusion and consequent disaster, all top enterprise executives need to stay in the compliance loop. Even if an internal audit group is charged with leading the day-to-day effort on Sarbanes-Oxley, the steering committee is a place where other, nonfinancial voices can be heard. This will eventually allow internal audit groups to save face when they realize that Sarbox is a much bigger job than they may have originally thought. Energen’s White, for example, is part of a seven-member planning group that includes the CEO, CFO, COOs of two subsidiaries, the HR chief and chief counsel. This group doesn’t just democratize communication, however. It also demonstrates resolve and commitment from the top. That’s crucial in most IT projects, but especially in Sarbanes-Oxley because, as Burlington Coat Factory’s Friedman puts it, “There is no value [in Sarbox] as far as the user community is concerned. If you don’t have executive pushdown on this one, people are not going to move on it.”

The Sarbox Compromise

Most auditors and CFOs we spoke with say that if IT is being left out of Sarbanes-Oxley, it is more a sin of omission, and perhaps ignorance, than a calculated plot. “The extent of IT

involvement depends on how intuitive companies have been about technology-enabled controls," says Mark Lindig, a partner with Big Four firm KPMG's IT auditing group. "If there isn't much understanding, then IT might not be there at the beginning. Finance looks at Sarbanes-Oxley and says: 'How can I do this from a numbers focus?' It's like a hub-and-spoke arrangement where finance starts it and brings in other groups as they go."

CFOs are also struggling with how to define other executives' roles in Sarbanes-Oxley. "Who signs on the bottom line?" asks Dennis Cavender, CFO of Essential Group, his voice shaking with emotion. "The CFO and CEO. That's who have to put their names on the line, and that's who it comes back to. I don't see Sarbanes-Oxley as a confrontation between the CFO and CIO; I see it as being a team that has to work closer together, or the processes and internal controls will fall apart."

CIOs could do everyone a favour by defining their role in Sarbanes-Oxley themselves. After companies get over the initial shock of discovering how many manual financial controls they need to document, the CIO eventually will be assigned to automate them to save time and expense in quarterly compliance efforts. "The CIO will become the custodian of controls," says Lindig. "The finance function has to own them because they are the last line of defence before the audit, but as the controls are distributed into the organization, you need to establish custodial and execution responsibilities. That's what Sarbanes-Oxley shines a bright light on. You have to have an accountability model for those controls."

This could be the natural role for CIOs — think access rights to systems, constructing employ portals, and other instances where the CIO already defines and manages automated controls. But it's a short step from there to a much larger role that many CIOs have been reluctant to contemplate: The move from simply owning and maintaining the IT plumbing to becoming accountable for the accuracy and integrity of the data flowing through those pipes — the data controller, as John Lenz, partner at consulting company Tatum Partners, puts it. "Just as we have financial controllers today who assure the accuracy and integrity of numbers, we will have data controllers who assure the accuracy and integrity of data," Lenz suggests.

Some CIOs have already accepted that accountability. Electronic Arts' West signs a certificate to his CFO that the data from his financial IT systems is accurate. The CFO and CEO are still ultimately (and legally) accountable if the numbers are wrong, but subcertification puts functional executives' necks on the line internally and in civil lawsuits. Gartner predicts that by next year, 70 percent of publicly traded companies will require their CIOs to do it.

CIOs who say they are currently satisfied with their role in Sarbanes-Oxley have one thing in common: They are defining their role themselves. They are volunteering to help coordinate the effort and offering project management — IT's unique, golden asset — to whomever wants it.

"I got involved and pushed the issue," says NStar's Zimon. "I thought, better to get involved early than have the business come to me with a list of demands [just before the deadline]." By turning Sarbox into a "project" like Y2K, and volunteering resources to staff it, Zimon got to have more input into the company's governance model. He also gained access to an early warning system that informs him of issues bubbling up. Now he's working on building a joint business and IT group to continue to monitor and support the financial controls after the first round of Sarbox passes.

"I talk to CIOs who say this isn't an issue for them like it is for me," says White. "I can't help but wonder if they aren't in for a rude awakening."

[Send Us E-mail](#) | [Privacy Policy](#)

Copyright 2004 IDG Communications. ABN 14 001 592 650. All rights reserved. Reproduction in whole or in part in any form or medium without express permission is prohibited.

written permission of IDG Communications is prohibited.