

Avoiding audit headaches

Keeping an eye on weak IT controls **Interviewed by Leslie Stevens-Huffman**

Many CEOs are aware that achieving Sarbanes-Oxley (SOX) compliance means they must consider the interrelated nature of accounting and information technology internal controls.

However, if CEOs take a deeper dive into the compliance pool, they may find that the company's policies and procedures, which are meticulously described on paper, don't actually mirror the firm's IT control processes that are enforced by the system.

Lee Barken, IT practice leader for Haskell & White LLP, says that user access controls are just one area that might need a review. As an example, Barken says that sometimes when he inquires about the company's purchase authorization limit for employees, he discovers that the IT system will accept purchase requests for far greater amounts than what is specified in the company policy.

With no carry-through of the company's policies into the IT control systems, a breakdown in controls can occur. User access controls are just one area that CEOs should be aware of when it comes to tightening internal control processes.

"CEOs can no longer just focus on dollars and cents at audit time," says Barken. "They must also think about zeros and ones when they set up and review their internal controls."

Smart Business spoke with Barken about the steps CEOs should take to avoid weak IT control processes and audit problems.

How can CEOs assure that company policies are reflected in the IT system and control processes?

First, check your software configurations and run numerous tests of the system to see if the company's policies match the system. For example, if you have a company policy that only allows certain users the authority to approve purchases up to \$100,000, log in as one of those users and see if the system will let you approve a purchase order for \$100,001.

Second, make sure all of your control processes and your tests are thoroughly



Lee Barken
IT practice leader
Haskell & White LLP

documented. Many chief information officers do a lot of things right, but they fail to document, and inquiry alone does not constitute a test of a control process. When the auditors arrive, they will want to see evidence that is documented.

Last, role-play some of the worst-case scenarios to make certain you'll be ready come audit time. For example, what happens if our CIO wins the lottery and disappears to a Caribbean island? Do we have policies and procedures documented? Will we have the proper documentation of the control tests and the results to provide the auditors?

Is testing and documentation of the company's data backup system required for an audit?

Having a clearly defined data backup policy is a vital control process because data loss can happen at any time, without warning, as a result of anything from a power loss to a natural disaster or even a simple mistake like someone accidentally deleting the wrong file. We learned a number of these lessons following Katrina and Sept. 11, so now auditors ask companies to provide evidence that the company will be

able to continue after an unplanned service interruption.

Data should be frequently backed up and the tapes should be stored off-premises as part of the control process. While the tapes are awaiting transfer, they should be stored in a secure and fire-resistant location. Keep a log that documents when backups are made and transferred and, on occasion, run a test of the restore process and document the results to demonstrate that you can restore the company to operating mode quickly. If you are storing tapes off-site, be certain to encrypt them, especially if they contain sensitive information, such as social security numbers or credit card information.

What type of network security documentation should be maintained for audit purposes?

Devices called firewalls control what information is allowed in and out of the company through the network. Firewall parameters should be established and tested in accordance with the company policies and procedures around information security.

With more wireless access to networks, how should control processes be established and documented for audit purposes?

Our traditional methods for securing the company's buildings and the information they house, like door locks and security cards, all go out the window when companies add wireless access to their networks. Think of encryption as the keys and access cards to your wireless network. Create a company policy about who can access the information and make certain that the data is properly encrypted with the appropriate encryption for wireless networks.

LEE BARKEN is the IT practice leader for Haskell & White LLP. Reach him at (949) 450-6200 or lbarken@hwcpa.com.

Insights Accounting is brought to you by Haskell & White LLP