Compliance Today - March 2022
Internal controls 3.0

By Gerry Zack


Gerry Zack

Please feel free to contact me anytime to share your thoughts: +1 612.357.1544 (cell), +1 952.567.6215 (direct), gerry.zack@corporatecompliance.org.

- twitter.com/gerry_zack
- linkedin.com/in/gerryzack

Early in the pandemic, when employees not directly involved in patient care were sent home, much was said about the importance of making modifications to internal controls in connection with compliance issues. Compliance professionals were wise to perform a rapid risk assessment to check on compliance vulnerabilities resulting from this sudden shift to remote work. Internal controls designed for an office work environment often need to be adjusted when employees are working from home. Failing to do so can create new compliance risks. I refer to this necessary shift as internal controls 2.0.

Now it's necessary to think of internal controls 3.0, resulting from a new hybrid work model. Many employees are now expected to work in the office some minimum amount but can work from home the rest of the time. This has the potential for doubling the nature or extent of some compliance risks. Another risk assessment is needed in order to gain a better understanding of this.

Think of it this way: As we went from internal controls 1.0 to 2.0, the shift went from controls needed to guard physical access to records or digital access from within the workplace to remote access to data through a VPN but with no access to the physical workplace, including access to records that would otherwise be available within the office.

In 3.0, we have a perfect storm. Employees have on-site access in the workplace *as well as* remote access through the VPN, and they shift back and forth between these two. Some businesses have long been accustomed to workers who travel extensively for their jobs, meaning they have always spent some of their time in the office and some of it on the road. But many organizations, and their internal controls, are not prepared for this hybrid workplace model.

We've already heard stories of employees, knowing they will be in the office next week, deferring certain tasks that will be easier to do in the office and, when they come into the office, accessing and downloading onto USB drives the files that they need when they work from home that might be more difficult to access using the VPN. Some are using personal devices to facilitate this.

Employees often find their own workarounds and efficiencies, rarely intending to weaken internal controls in the process. But in doing this, they may expose vulnerabilities in a system designed for a different work environment.