ControlPanel GRC

SYMMETRY™

The Top Five IT & ERP Compliance Issues Smoldering Beneath the Surface

When firefighters arrive at a burning building, their first priority (of course) is to knock down the visible flames. Yet experienced firefighters know that when those flames are extinguished, the job isn't done yet. That's the time they go in and start looking for the hidden flames – the smoldering materials in a ceiling or behind a wall that could suddenly erupt and engulf them when they're not expecting it. They know those hidden fires can be the most dangerous of all simply because they can't be seen until it's too late.

For the past few years, IT and compliancemanagers have been like those firefighters first arriving on the scene. You've been putting out the compliance fires – the big issues that have been burning brightly since SOX legislation was passed in the early part of the millennium. You've done a good job too, creating a new compliance structure where roles are defined, segregation of duties (SOD) is the standard and transactions are well-documented.

Yet just like those firefighters, the job isn't finished yet. There are still all kinds of compliance issues that, while not as visible as thefirst ones you tackled, can still create a back-draft that will burn your organization if you're not careful.

Following are five of the most pressing (and potentially dangerous).

ControlPanel GRC

SYMMETRY

1. Excessive Access

With the complexity of the security architecture that is part of modern ERP systems, it's easier than you might think to accidentally give some users access to potentially sensitive transactions that might be far outside their job descriptions. Access is usually assigned by the help desk, and in the heat of battle, with many pressing issues, they may not be as careful about assigning or doublechecking authorizations as they should be. When that occurs, it can lead to all types of dangers. Imagine a parts picker in the warehouse being given access to every SAP® transaction in the organization (which has happened, by the way). In that instance, the warehouse worker started running and looking at transactions (including financial transactions) just out of curiosity. But what if he'd had a different agenda? He could have changed the data, either accidentally or maliciously, or executed a fraudulent transaction, creating a serious compliance breech.

Excessive access is not the type of issue that will show up in a SOD report.

Even if he didn't change anything, there's still a productivity issue. After all, if he's busy running a myriad of transactions, he's not busy picking orders.

Excessive access is not the type of issue that will show up in a SOD report. The best way to address it is by installing governance, risk and compliance (GRC) software that makes managing security and authorization easier. The software should also provide you with tools that help you measure and monitor actual system usage so you can see whether the things users are doing and the places they're going within the system are appropriate to their job requirements. Having automated systems in place is particularly important in smaller enterprises that usually do not have the resources for a lot of manual inspection.

2. Access to Sensitive Data

Users don't necessarily need access to a broad variety of data to pose a risk; they just need access to particular data. For example who can open and close posting periods. Who can view HR salary and benefits information? Again, this is nothing that is likely to show up on a SOD report, yet it's a very real risk.

We've all heard the stories about how a certain soft drink manufacturer's formula is betterguarded than the launch codes for nuclear weapons. Imagine if the formula was sitting on the ERP system and the wrong person was given access to it – or given access to payroll, HIPAA or other sensitive information.

ControlPanel GRC

SYMMETRY™

One key to controlling access to sensitive data, of course, is to exercise more care when assigning authorizations. This is called preventative controls. It's also important to use reverse business engineering tools to see who does have access to sensitive transactions, whether that access is appropriate, and what they did with the information once they had it. This is called detective controls. It's like following the smoke to discover where the hidden fire is.

3. Poor Segregation of Duties

Although SOD has already been mentioned, some organizations are not familiar with what it is and its purpose. Let's look at the nuclear missiles analogy again. In order to launch, there are two keys controlled by two different people. Two keys are used to assure that no one person has control of the missiles in case someone decides to "go rogue."

SOD conflicts are unavoidable making a tool that can monitor actual transactions and report violations essential.

It's the same with financial transactions in an enterprise. You don't want one person to be able to create a vendor in your SAP system and then initiate payment of that same vendor; you're just asking people to steal from you.

That's why it's important to have value-added tools that analyze user access against the enterprise's SOD rulebook and flag any conflicting functions. An ongoing analysis will point out any areas of risk so they can be remediated, and keep you informed should the situation change.

Of course, in a smaller organization, conflicting duties may not be avoidable. Everyone is expected to wear multiple hats, and sometimes those hats do not allow for proper segregation. In those instances, you need to have tools that can monitor actual transactions and report against them so you can see if a compliance violation is occurring. In other words, if someone has to carry both keys, you know when they've inserted them both into the control panel through mitigating controls.

Even with the proper tools, it's unlikely you'll ever bring SOD conflicts down to zero. But you can get awfully darned close, and keep an eye on what happens from there.

4. Introduction of Malicious Programs into Production Systems

The modern reality is that ERP systems are rarely steady state.

Often enterprises have multiple initiatives going on that introduce new data, configuration and programs into the production systems. With lean staffing and urgent deadlines, often changes are not properly tested or audited. In other wthey don't use

proper change management. A developer who has the means to do it, the motive to do it and knows whether he/she can get away with it can wreak all kinds of havoc by including malicious code along with legitimate code when new applications are moved into production. Malicious code can download sensitive data, create fraudulent transactions, delete data or crash the systems.

Poorly coded, untested programs can result in a catastrophic outage making adherence to change control processes vital.

It is critical to have a second person reviewing any changes at every step of the way. What that means is the person who requests the change can't be the person who develops it; the developer can't be the person who tests it; the person who tests it can't be the same person who migrates it into production. In other words, transport development and approvals cannot be given by a single person – instead, an independent approver or even a committee must be controlling the entire process.

Change management duties need to be segregated and managed throughout the entire process. Even if not malicious, poorly coded, untested programs can result in a catastrophic outage. Given that in a large enterprise an hour of downtime can cost $1 million, it's easy to see why proper change management is worth the investment.

5. Emergency Access

In large ERP environments, there's always the chance that emergency maintenance of production systems will need to be performed. When it does, and the enterprise is dialing 9-1-1, someone needs to be given emergency "super user" access to everything in the system. Such emergency maintenance is often by outside parties (e.g. the software vender or 3rd party consultants).

The problem is these emergency all-access passes aren't always tracked very well. Everyone is so fixed on putting out the fire – for example unlocking a sales order that has frozen the entire system – that they never think about documenting what transactions were performed or what data was changed. The risk is increased by the widespread use of generic "firefighter" user IDs whereby the individual performing the actions isn't definitively known.

You'd like to think that the person you give super user access to can be trusted. But blind trust is what has gotten other enterprises into trouble in the past. The person with full access may make other changes while he/she is in there – either accidentally or on purpose. You need to be able to monitor who has all-access and what they do while they have it.

About ControlPanel[GRC]

ControlPanel[GRC]™ is a new breed of Governance Risk and Compliance (GRC) automation solutions – one that focuses on rapid implementation, ease of use and broad functionality aimed at making SAP® users Always Audit Ready™. Part of Milwaukee-based Symmetry Corporation, ControlPanel[GRC]'s integrated GRC technology suite addresses the major areas of compliance concerns for SAP users. With over 50 implementations in two years, ControlPanel[GRC] has given its clients the ability to confidently satisfy compliance requirements while accelerating workflows that enhance their team's productivity.

For more information about ControlPanel[GRC], visit Symmetrycorp.com or call 1-888-SYM-CORP.

Always Audit Ready™

It is critical to have tools that allow you to track what these super-users do while they're in the system. Not just for the day-to-day operation of the business, but for the auditors as well. When auditors see someone has been given this additional emergency access, their job is to immediately assume the person did something nefarious. It will be your job to prove they didn't. You'll need to show why access was granted, what was done while the person was in there, when/how long the person was in the system, what changes were made and when the person exited.

While it's important to put out the big compliance blazes, keep in mind those are the ones that are also easy to see. Once they're under control, take a tip from the professional firefighters and be sure to check for the smaller, smoldering flashpoints.

It's your best insurance against getting burned.