FASTPATH

SAP® Access Controls: Protect Your Company from Fraud - Know the 5 Ws

The Why, What, When, Who and Where of Access Controls

FASTPATH

SAP Access Controls: Protect Your Company from Fraud

The Why, What, When, Who and Where of Access Controls

Everyone in your company can definitely trust everyone else in your company.

Unfortunately, this statement is not a reality for most companies. If you believe it's true for yours, then you may not need to finish reading this paper.

However, if you recognize that people are people, you'll know that anyone can be pressured into doing things they would otherwise find unimaginable, like stealing from their own company. Besides, you owe it to your stakeholders to make certain that your company's highly valuable financial and information assets are thoroughly protected from attack or theft from outside your company, and from within.

Why Access Controls are so Important in SAP

SAP is used to operate many of the largest companies in the world, as well as midsized and smaller ones. No matter how large the company, multiple people in different roles will need to enter and obtain information by interacting with SAP. However, not all of the people in all of those roles should be able to access all of that information. Financial personnel will likely need access to financial data, but not operational data. Inventory control people will only need information pertaining to inventory.

The goal of access controls is to provide each individual in each role in the company with the minimum rights they require to do their work, and nothing more.

Unfortunately, in some companies those who originally set up SAP simply gave all rights to all data to all personnel in all roles. It was just easier and quicker, and it instantly created as much exposure as a company could possibly suffer. Imagine an employee who becomes unhappy with the company using their unlimited or "administrator" rights to simply delete all data and backups. They could cripple the company with a few keystrokes. This may be extreme, but think about all the harm that could be caused at any time depending upon the whims of human beings.

No company can afford that. That's why access controls are so important in SAP.

What Needs to Have Controlled Access?

The simple answer is everything.

Every feature and function within SAP contributes to one or more processes that the company must perform regularly to operate. Each individual has a specific role that exists at one of several levels. Department managers, for example, need access to most processes related to their department. The people who report to them however, only need access to the functions that support their specific job function. They shouldn't be able to access performance reports for the department, or everyone's personal information.

Access control becomes even more important in the context of regulatory compliance. Many companies must comply with various government regulatory acts or face punishment including heavy fines. Just about every one of these acts not only requires the implementation of various measures to assure the safety and privacy of data, they also require documentation that the measures are performing effectively.

Without access controls to enforce the policies and procedures required, there can be no assurance of regulatory compliance.

When are Access Controls Important?

Whenever a user logs into SAP they must authenticate themselves by providing an ID, a password, and usually some other proof of their identity. Once they are authenticated, the access controls immediately work to limit the resources that user may access.

For the entire time that the user remains logged into SAP, the access controls continuously assure that they cannot access any data entities or system processes for which they do not have approval.

Who Needs Access Controls?

Ultimately, anyone who owns fiduciary responsibility to protect the company's most valuable assets must know at all times that access controls are in place and fully up to date, to assure that the only people who can access specific data entities are people who have been approved to do so.

Since it is virtually impossible to look over everyone's shoulder to see what they're doing at all times, automated access controls are the only way to provide complete and comprehensive assurance.

Where Are Access Controls Needed?

When so many users are accessing SAP from a mobile device that may be located anywhere, access rights must become even more granular. Not only are they assigned by role, but the same user may have certain rights that are only available when they are physically on the company's premises, not when they are operating remotely.

The ultimate goal is to provide secure access to any data, on any device, across any network, at any time or place, but with the appropriate access controls. These controls limit what data, what devices, which networks, and what times and places are acceptable.

Best Practices for Access Controls in SAP

Do Not Address Access at Role Level

Access Controls in any system need to be designed to detect risks that can undermine all of the automated processes management relies upon to prevent and detect material misinformation from being applied to the financial statements. This is accomplished by reporting on the most root level securable objects, which in SAP is typically the authorization object.

Attempting to address access at the role level cannot be relied upon. Roles can be designed to do almost anything and often are, especially if fraud is a concern. The name of a role can be virtually anything the user chooses as it is a free text field. You can label a role something along the lines of "Keith's role that definitely, most assuredly, contains no risky transactions". That particular name may lead one to believe the opposite, but it is still a valid role label.

Put Security First (or Even Second - Just Not Last!)

During an SAP implementation process, security should be one of the first and most important elements to address. Unfortunately, most often it is ignored until the last possible moment. Most SAP implementations will engage a system implementer, but it's worthwhile to note that most system implementers preclude themselves from advising on risk. These advisors will implement the process that the business tells them is necessary and the security that is needed to allow themselves to perform those functions.

Audit requirements and risk around segregation of duties and sensitive access will usually not be considered during this process. In order to get this initial setup correct, the business process owner, risk owner, and system designers should all be included in the analysis.

Using Least Access for Maximum Security

In SAP, users should be granted the least amount of access necessary to perform their specific tasks. This is difficult to design, especially when starting in an inclusive initial implementation as described above. After the implementation, the typical SAP instance will deprecate rather than improve.

Next steps relate to the request for, and the provisioning of, additional access to users. This is most often done by granting new roles rather than editing current roles as that process can be quite time consuming and difficult, leading to additional problems. This is why role redesign projects have a tendency to come soon after implementation, and can be costly and time consuming.

During the implementation process access should be addressed at the lowest securable object level and granted on the basis of least-access-necessary. In order to accomplish this, there should always be a business process design meeting to scope and identify risk associated with the process. This meeting needs to include all the parties who are involved in the process in order to determine the details of who needs what security. The accumulation of all these areas will lead to development of business roles that allow users to perform the tasks necessary, but not significantly more.

Common SAP Access Control Issues

Custom Code

SAP offers some significant issues from an access controls perspective, the first of which is one of the biggest pain points around customizations. Custom code in SAP can and almost always does, undermine the basic security structure setup by calling additional access and effectively allowing users to perform tasks for which they were not approved to be provisioned. Customizations can be written in many different ways including custom T-codes, direct BAPI calls, direct table calls, and more. The important piece is being able to catalog all of these customizations, understanding what they actually do, and including them in the risk analysis related to security.

The transaction log in SAP will report every time a particular T-code is executed, whether that transaction was executed by an individual directly or whether it was called. That called transaction can come from a native T-code in SAP, a custom T-code built specifically for your business, or a partner-developed application that is integrated. When running a transaction log of FB05, paring down the scope of how many and by whom those transactions had to be reviewed is important.

Under a certain threshold most transactions are immaterial and not subject to multiple reviews. Therefore, it is difficult to determine the source of many small dollar value postings. Sometimes connecting alternate applications to SAP can lead to a multitude of small dollar value transactions that are impossible to separate from transactions made directly in SAP by individual users.

* Organizational focus on controls rationalization and minimizing testing costs has increased over **60%** from 2017-2018.

SAP can be an incredibly powerful application for processing transactions. It can also be very difficult to control what happens in SAP without the proper internal controls and ongoing monitoring process. As it applies to security, you should regularly analyze users and roles for segregation of duties, sensitive access, and changes made without approval. When the initial implementation is done correctly, including the proper scoping and mapping, least access necessary granted, and changes monitored in an ongoing fashion, you can prevent ending up in a role redesign process.

Cross-Platform Access Controls

Another common issue becoming more and more prevalent in the marketplace is cross-platform access controls. While SAP offers supporting products in most different areas, users are more often buying best-in-breed applications and plugging them into SAP. It is less and less the standard practice to simply "follow the logo" and apply all SAP applications.

Even if the ecosystem includes only SAP applications SAP now owns through acquisitions, some platforms written in JAVA rather than ABAP, which adds difficulty because their native GRC application does not operate with all of them.

Process Outline – Initial Process

One of the reasons that access controls have become as important as they are stems from the attitude among early system users that many subsystems were "set-it-and-forget-it", meaning that once the access controls were set up, they would do their job without attention.

The world is far more dynamic than that, and the access and processes required may change often. Access controls must be just as dynamic, with far more careful control. Especially in as fluid an environment as data networks are, vigilance must be constant. Effectiveness of your access controls must constantly be monitored and adjusted.

This ongoing process begins with the initial processes required to set up access controls in the first place. Once established, none of these processes is at its end. There will be ongoing processes in place to assure that every access control is doing what it was designed to do, and all assets and processes are safe.

* From the KPMG 2018 Internal Controls Survey

These initial processes include:

Setting Up Security:

Before you can set up security, you must know and fully understand what you are securing. To accomplish this, you must execute an exhaustive inventory of everything that is involved in running SAP:

- Identify every data asset. For each, determine its value, the risks involved in case of corruption or theft, the materiality of each which helps determine how much should be spent securing each, and which SAP modules access each.
- Describe every role that a user may play in the organization, identifying which SAP modules they use and which data assets they must have access to.
- Identify every user, including which department they are in and their position description.
- Map out business processes and flowcharts to fully define each process and how each relates to involved data assets and user roles.

Assigning Security

- Now that all roles have been defined, each must be assigned the appropriate access rights for anyone in that role.

Designing a Ruleset

- The rules governing access to specific data assets are often conditional. For example, all users may be prevented from accessing many resources during an audit. Some procedural steps must be completed before access to certain resources may be granted. These conditions are represented in a ruleset that governs all related processes.

Provisioning Process

- Now that you've identified all your personnel, all the roles each may play, and assigned specific access rights to each role, it is time to assign each person to a specific role.
- By assigning each person to a role, you won't have to revisit each user every time there's a change in operations to adjust their access rights. You can manage the roles which will make the necessary adjustments for all users within that role.

Emergency Access

- Emergency access is a role that gives the user sufficient rights to handle any unusual circumstance that may arise. Since this means fairly broad access, it should only be assigned temporarily to very few users who are required to resolve whatever emergency may arise. It is also critical to establish policies that remove users from Emergency Access once the situation is resolved.

Process Outline – Ongoing Process

Systems are dynamic entities that must change constantly. As they do, the controls needed to preserve safety and privacy change along with them.

The safety net for your organization rests with the Audit department, your internal auditors whose primary goal is to assure that you are always prepared for external audit. Audit has a seat at the CFO's table, making them the risk-mitigation stopgap required to apply the brakes whenever the system veers off course.

As the concept of DevOps has emerged where software developers and system operators work in concert using similar tools and processes to assure smooth operation and continuous improvement, "AudOps" must do the same. Here, the Audit department collaborates proactively with Operations departments to assure that all access controls are in place and performing their task.

One of the most intricate projects you will undertake will be the periodic "role re-design" that may result when various roles and departments cannot be re-certified.

Segregation of Duties (SoD) Analysis

For SAP to be as powerful as it is, it stands to reason that it must also be significantly complex. In the context of vital access control, this means that some of the capabilities assigned to specific roles may inadvertently conflict with company policy. As an example, there is inherent risk in allowing the same person to create a new supplier on the system, request payment to that supplier, and then approve their own request.

Because it is all too easy to create conflicts like this, it is critical to perform regular Segregation of Duties reviews so you can identify these flaws and correct them.

Risk Management

In the context of ongoing operations, there are some particular risks to pay attention to. As time goes on and people make various changes in the system, it is always possible to re-establish conflicts that were already resolved or create new conflicts. The best way to manage this is to perform regular reviews to assure that no conflicts exist. Again, there's no room for "set-it-and-forget-it" thinking.

Another major area for risk to arise is in the management of users. When people are dismissed from the company, often there is insufficient attention paid to the need to remove all their access rights and their identity on the system, during the offboarding process. This can wreak havoc when a dismissed employee decides to take revenge by using their still-active access to damage or destroy entire datasets and workloads.

Recertifications

It is important to periodically re-visit all users to ensure that they have all the access rights they require, and only the access rights they require. In too many cases the manager of a group of users may simply "rubber-stamp" such a re-certification, but they are disserving themselves, their employee, and their company when they do so. Everything changes constantly, and access rights are constantly impacted by those changes. This makes periodic re-certification critical.

Reporting & Documentation

Audit is one of the most valuable processes in any business. Audit motivates everyone to keep everything within established parameters and document their success. Relevant reporting is the most important tool to help everyone remain fully prepared for an audit at any moment in time. This is similar to having regular medical check-ups. You want to make sure everything is working well to avoid complications later on. You're willing to endure some discomfort to gain this assurance.

Look upon auditors, internal or external, as your very best friends. They help you be prepared at all times to deliver optimal service to your company. Reporting that helps you be so prepared is the only kind of reporting you need or should accept.

Advantages of Automation

In the course of this paper we've discussed several processes including segregation of duties, role recertification, and various kinds of audits. When you think about the complexity of all of the rules governing all of the roles in the context of thousands of processes you almost immediately realize that it would be virtually impossible for a human being to review everything and make the correlations required to correct errors in a reasonable amount of time.

Automating these processes is mandatory. It is truly the only way to interrogate everything that needs to be examined and perform all the tests that reveal existing conflicts. Many system managers attempt to catalog everything in Microsoft Excel and regularly compare their data to a given ruleset. Anyone who has attempted this will almost certainly agree that automation is indeed required.

* Organizations cite their largest area of improvement is related to technology and control automation. **71%** of organizations are looking to increase improvement in these areas.

Conclusion - Get Your Risk Under Control Now

The importance of maintaining vigilance and constantly reviewing and revising your access controls grows with scale. The larger the environment, the more complex it becomes. The more complex, the easier it is for conflicts to occur. The more conflicts occur the greater your risk, and therefore the greater your need for proactive management of all access controls.

One solution that helps build great efficiencies is the Fastpath cloud-based application focusing on cross-platform access controls. With native connectors to SAP as well as many ERP, CRM, HCM, and other applications, Fastpath addresses access controls from a business process perspective rather than by application. It also helps SAP customers automate the identification and logging of custom code through application of its code checker, specifically built for SAP. Through the use of these automated tools, users monitor security continuously in an automated fashion, which not only leads to great efficiencies but also helps to prevent the time-consuming and costly process of role redesign.

About Fastpath

Founded in 2004, Fastpath has deep expertise in audit, security, and compliance, with multiple Certified Internal Auditors on the team. Fastpath has global partnerships with several audit firms and a client base which spans across multiple industries within both publicly traded and privately-held companies. Fastpath Assure® is a cloud-based audit platform that can track, review, approve and mitigate access risks across multiple systems from a single dashboard.

Contact us to discuss your needs or for a product demonstration. Visit our website for additional resources like this eBook, on-demand webinars and more.

* From the KPMG 2018 Internal Controls Survey