

Building More Effective Access Control Through Business-Centric GRC

IF YOUR SAP ROLES AND
RULE SETS ARE SOUND,
YOUR ACCESS CONTROL
SOLUTION IS SET UP FOR
SUCCESS.



Craig Powers

Research Analyst, SAPinsider

Companies utilize access control solutions to identify risk within their user base. These solutions and processes are often technical and driven from audit and IT perspectives with very little input from business users who might find the technical GRC language hard to decipher. That's where the idea of business-centric GRC comes into play for access control—providing the business with easier to understand, less technical language so that they can better interpret the data.

“If business users understand access risk, they are more likely to ultimately take ownership of it,” says Dudley Cartwright, Managing Director and Co-founder of Soterion, a company specializing in SAP access control solutions and associated SAP security services.

When the business users take ownership of access risk, they can be held accountable. Cartwright says creating business-centric access control is difficult to do internally and requires a solution that speaks to business users, such as Soterion's Access Risk Manager, which features user-friendly interfaces and business process flows for easy risk remediation and effective access control management.

Building a Solid Access Control Foundation

While it may take the right business-centric GRC solution to get business users invested in access control, Cartwright warns against viewing the software as a silver bullet. First,



correcting the SAP role design within SAP must be done to optimize any technology investment. Once the SAP roles are in place, companies must then ensure their GRC rule set is customized to align with their unique access and risk requirements.

If your SAP roles and rule sets are sound, your access control solution is set up for success. The question then becomes: How do you measure success in access control? Cartwright says it should be measured by how well business users carry out access risk management activities. That again emphasizes the need for having business user engagement.

"A lot of companies implement GRC solutions, and business users need to perform certain of these GRC functions, but they understand very little about GRC itself," explains Cartwright. "They complete the tasks to tick an audit box rather than to address a specific need within the organization."

Top Access Control Requirements and Strategies

What are organizations looking to achieve with an access control solution? First, says Cartwright, they need to ensure that their SAP systems are secure, often driven by internal and external audits. These audits seek to monitor if people are

KEY TAKEAWAYS



Business-centric access control engages business users in the access risk management process to help align access better with business needs.



SAP role clean-up and GRC rule set customization are vital foundational elements to a successful access control solution.



Companies can significantly reduce access risk and access overallocation through greater business involvement in access control.

COMPANY SNAPSHOT



SOTERION

Soterion focuses on building business-centric GRC solutions that enhance business accountability of risk within SAP systems. Soterion provides GRC solutions that work on-premise, hosted, or through managed services based on an organization's needs.

assigned appropriate access and determine fraud risk associated with improper access.

Companies are also concerned about improving efficiencies of their SAP user provisioning processes and making it easier to manage authorizations. The goal is to get business users to perform compliance tasks and access risk management activities much more efficiently.

Complying with regulations is also a top priority for implementing access control processes and solutions. This requirement is particularly important for data privacy.

"There is an incredible amount of sensitive personal data in SAP," says Cartwright. "Understanding where that data resides and who has access to it is important—especially when complying with data privacy regulations."

Finally, Cartwright says companies see the need to move access risk responsibility away from IT departments and to business users. This shift means moving beyond using GRC solutions solely as back-end tools and becoming more business-centric in managing access risk, as he has described previously.

To accomplish these objectives, companies are looking at streamlining provisioning processes and utilizing automation to improve efficiencies. One example is using a password self-service application that enables end-users to automatically reset their passwords, which will help to reduce support costs.

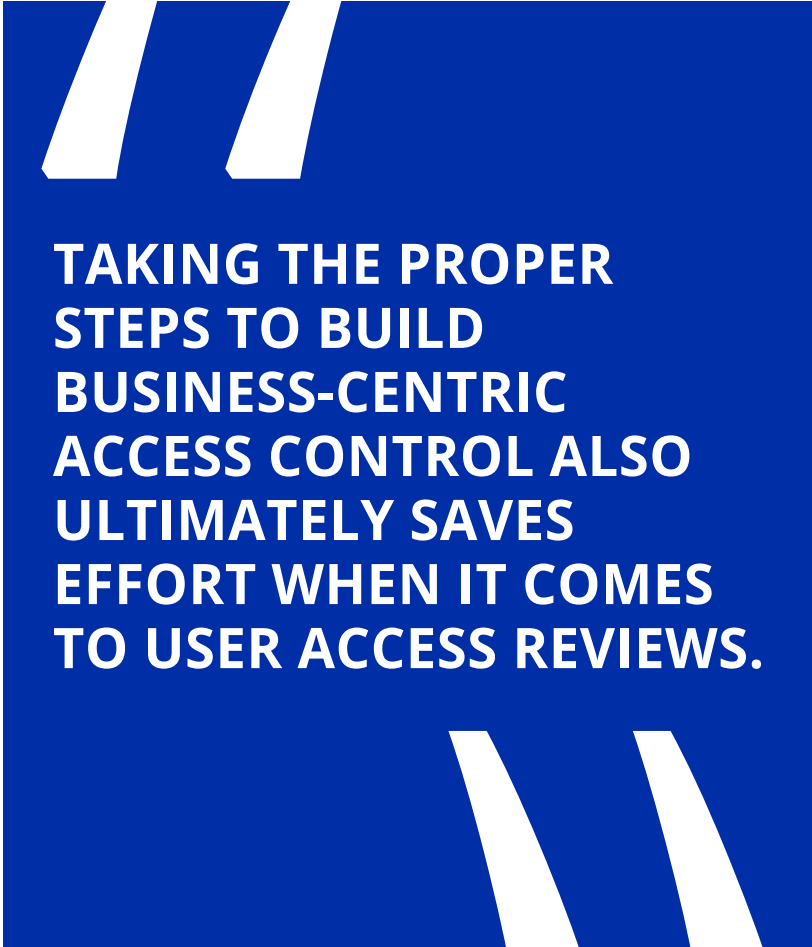
Benefits of Business-Centric Access Control

Cartwright says his clients tend to use KPIs that measure how much access risk is in their systems and if GRC solutions improve the audit process from year to year.

He has seen organizations reduce access risk by as much as 80%, significantly minimizing the potential for fraud. One way business-centric access control reduces risk is that business users make informed decisions as to whether their users need specific SAP access or whether it poses too significant a risk to the organization. This informed decision-making process results in only assigning only appropriate access to the users, which reduces the potential for fraud in the organization.

"By aligning access with what users are doing, you tend to reduce overallocated access, which is common in SAP," says Cartwright. "As people move around an organization, they inherently are given more access as time goes by."

Taking the proper steps to build business-centric access control also ultimately saves effort when it comes to user access reviews. So much of the access clean-up has already been done in building a strong solution, Cartwright explains, so when the actual access review occurs, the business users save time and effort.



**TAKING THE PROPER
STEPS TO BUILD
BUSINESS-CENTRIC
ACCESS CONTROL ALSO
ULTIMATELY SAVES
EFFORT WHEN IT COMES
TO USER ACCESS REVIEWS.**

WHAT DOES THIS MEAN FOR SAPINSIDERS?

Based on Cartwright's insights into business-centric GRC and access control, SAPInsiders should consider the following recommendations:

1

Properly defining your SAP roles and GRC rule sets are essential. If your SAP roles and GRC rule sets aren't adequately set up and customized to your organization, it becomes difficult to assign appropriate access. If that's the case, it doesn't matter how great your GRC solution is because it won't correctly assess risk without accurate role and rule set data.

2

Make access control accessible to business users. While many companies rely on IT to carry out access control through GRC software, the business users must carry out proper access risk management processes. Provide business users with user-friendly interfaces and easy-to-understand (read: non-technical) language around necessary risk management. They will be more engaged and more likely to limit access risk effectively.

3

Go beyond audits when measuring GRC effectiveness. It's tempting to rely on audits to do the heavy lifting when it comes to measuring the effectiveness of your GRC and access control programs and technologies. However, that's more of a measurement of the result, not the process. Companies can get ahead of audits by looking at how well business users are performing their access risk management duties along the way.