Moving to SAP® S/4HANA? Don't Leave GRC Behind

Introduction

As organizations are preparing to move to SAP® S/4HANA, SAP's latest platform, an important step in their journey to a more secure and compliant SAP environment is upgrading — or in most cases, enhancing — SAP Access Control.

In this paper, we review the changes organizations need to make to their governance, risk and compliance (GRC) road maps when preparing to move to S/4HANA. In addition, we summarize several new enhancements by SAP to the Access Control environment. The enhancements were based on direct customer input, and organizations are advised to take advantage of these new features as they move to S/4HANA.

SAP's Focus on Cloud and S/4HANA

SAP® S/4HANA brings significant capabilities around analytics, reporting and simplified accounting processes, and is architected to connect people, devices and business networks in real time by enabling flexibility of applications to be used on desktop computers, tablets, and smartphones.

SAP has published a road map outlining the company's long-term plan for the cloud version of the software. The road map outlines future integration with other SAP cloud applications, such as SuccessFactors, Concur, Ariba and Fieldglass. Further, SAP has introduced

native connectivity to SuccessFactors as a first of many recent enhancements allowing connectivity to SAP's cloud-based applications.

Many organizations are beginning to understand the value of these improvements and are developing plans for a migration to, or implementation of, S/4HANA. However, the move requires organizations to evaluate carefully the complexities of their future ERP landscape, including the integration of their other business-critical applications into the cloud and ensuring that the upgraded ERP environment is compatible with the organization's existing Access Control environment.

How Will S/4HANA Affect the Current GRC Environment?

The S/4HANA architecture introduces complexities to the GRC environment resulting from the new and updated functionality, HANA database and Fiori front-end server (optional). The new HANA database and Fiori front-end raise important questions about security, including how to provision access to both Fiori and the HANA database, segregate conflicting responsibilities across systems, and manage temporary elevated access. Enhancing or enabling the Access Control functionality should be considered as part of the S/4HANA implementation. Some questions to consider include:

- Are there new access risks or changes to existing access risks?

- How will additional systems (HANA database, Fiori) be integrated to ensure a complete and consistent provisioning process?

- How will elevated access be managed in the S/4HANA, HANA and Fiori systems?

- How will existing security architecture and ownership change as a result of SAP's role-based user experience strategy?

Leveraging the HANA Database With SAP Access Control

The expanded and broader use of the HANA database will prompt organizations to think more broadly about how to take advantage of the in-memory database and achieve more advanced reporting and analytics capabilities. While many organizations may already be taking advantage of HANA to improve performance for Business Warehouse (BW) reporting, HANA offers even more. One of the more obvious benefits of implementing SAP Access Control on HANA is the performance gains realized around the risk analysis functionality. The use of HANA with SAP Access Control also enables several Fiori analytical and factsheet apps, which provide quick access and insight into the GRC environment.

Integration of the New S/4HANA Architecture With Access Control

Moving to S/4HANA means that the new architecture will have to be integrated into the company's existing Access Control environment. The ability to perform risk analysis and user provisioning activities to the HANA database has been available since the introduction of Access Control 10.1. With Fiori and HANA, end users may need access to additional security roles on the Fiori and HANA systems. Enabling provisioning functionality to these systems is imperative to ensure a consistent end-user experience and allow access to be requested and provisioned utilizing existing automated processes.

What Are Some Recent Access Control Enhancements?

SAP continues to innovate and introduce enhancements for the SAP Access Control application through quarterly support package releases, and companies should take advantage of these enhancements as their IT departments work to integrate Access Control with the S/4HANA platform. We reviewed the recent updates and have summarized some of the key enhancements here. These recent updates and enhancements were introduced by SAP as a result of direct feedback from customers.

Native Integration with SuccessFactors

In March of 2017, SAP introduced a significant enhancement that enables native out-of-the-box integration to connect and provision access to SuccessFactors. This is the first of many steps by SAP to integrate cloud-based applications in their current portfolio with other SAP applications. With this recent enhancement, many organizations should revisit their GRC roadmaps and evaluate integration to other non-SAP applications by kick-starting user provisioning connectivity to SuccessFactors. This functionality can be made available on its own via implementation of an SAP note[1] or through an upgrade to support pack 17.

[1]   SAP Note 2408333, "Enable Provisioning of SuccessFactors Users in SAP Access Control."

Improvement in Simulating SoDs

GRC risk analysis simulations at the role and user level now have the option to perform both assignment and removal of objects (roles, profiles, authorization objects) during the same simulation. Prior to this update, organizations could not include assignment and removal in the same simulation (i.e., replacing a user's role with a new role for the purpose of simulating SoD or critical access risks). Additionally, SAP has added a feature allowing users to import a list of roles into a simulation rather than selecting roles one at a time. This is a key enhancement, as many organizations struggled with simulating large changes to a user's access.

Reporting Enhancements

A number of new reports have been created in SAP Access Control that will assist organizations with more visibility into where users are receiving their access. It is clear from this enhancement, which is based on user feedback, that more organizations are leveraging the business role functionality. Some of the updated reports include:

- User-to-business role mapping

- Comparison of two business roles

- Comparison of two users

- Business role-to-transaction mapping

Additionally, risk analysis dashboards now allow the use of wildcards or multiple selections when filtering by user group (previously only single user group selection was allowed). Ad-hoc risk analysis can have a default report format configured in SAP Access Control (previously the non-configurable default was at the summary level). Finally, the Action Usage Report can now analyze role utilization by users taking into account the same historical transaction code usage data that is used in user access review forms.

Firefighter ID Management and Automated Reviews

Firefighter ID management continues to be a challenge for most organizations. Currently, this functionality supports assignment and management of the IDs; however, to date, there has not been any functionality to review the assignments, resulting in incorrect assignments, need for clean-up activities, and unmanaged risk. Many organizations assign Firefighter IDs to users for an extended period of time (or indefinitely). Performing a periodic review of the Firefighter IDs assigned to end users, similar to reviews of roles assigned to end users, can serve as a control to reduce the risk of inappropriate elevated access. This most recent enhancement allows an automated review to be configured as a new workflow in SAP Access Control.

User Access Review

The User Access Review functionality received two new enhancements. The first update relates to users affected by access changes as a result of the access review process. These affected users can now be notified if a reviewer requests access to be removed during the review process. Previously, only individuals involved in the access review workflow were available to be notified. This enhancement will increase transparency for the users during the access review process and reduce helpdesk requests from users after having roles removed.

The second enhancement allows the user's manager to now be included in the review form during a role owner's user access review. This feature will assist role owners by giving them a point of contact for additional information regarding a user's access prior to making a decision.

Improving Access Request Submission

Similar to the import feature added to risk analysis simulations, roles can now be uploaded into an access request form instead of having to be selected manually. This enables organizations to reduce the level of effort during the access request role selection process and allow requesters to upload common role combinations through the use of predefined sets of roles (similar to templates) which they can now upload directly into the form.

Security Changes for Access Request Templates

Access request templates are part of the existing functionality and an effective way for users to start with a predefined, standard access and modify it prior to submitting the request, often by removing unneeded access prior to submitting. Until recently, access request templates had limited security restrictions. In the most recent enhancement, organizations are given a greater level of control over access request templates through the introduction of authorization objects specific to the request templates that allow restrictions on creating, modifying or deleting request templates. The documentation of the security updates is now available in the GRC Security Guide published by SAP[2].

In Closing

The SAP Access Control enhancements outlined above are just several of many that are becoming increasingly relevant when evaluating a change in the ERP landscape as result of digitalization or other transformational activities. Changes of this magnitude are accompanied by risks that need to be managed before, during, and after transformation. Moving to S/4HANA presents not only a technical change, but introduces risks associated with migrating to the cloud, moving to a new database platform, increasing business user engagement using additional user interfaces and devices, updating existing business processes through new functionality, and ever-multiplying integration points with the new financial system.[3] Organizations must stay ahead of these risks by not letting security and GRC become an afterthought in the planning for their move to S/4HANA.

Contacts

Toni Lastella – New York
+1.212.399.8602
toni.lastella@protiviti.com

Carol Raimo – New York
+1.212.603.8371
carol.raimo@protiviti.com

Aric Quinones – Atlanta
+1.404.240.8376
aric.quinones@protiviti.com

Thomas Luick – Chicago
+1.312.476.6342
thomas.luick@protiviti.com

John Harrison – Houston
+1.713.314.4996
john.harrison@protiviti.com

Steve Cabello – Los Angeles
+1.213.327.1470
steve.cabello@protiviti.com

Ronan O'Shea – San Francisco
+1.415.402.3639
ronan.oshea@protiviti.com

Martin Nash – Tampa
+1.813.348.3374
martin.nash@protiviti.com

---

2   Available at https://websmp107.sap-ag.de/~sapidb/011000358700000596352013E (login required).

3   See Protiviti's white paper, *Understanding the Responsibilities of the Business During an ERP System Implementation*, at www.protiviti.com/US-en/insights/understanding-responsibilities-business-during-erp-system-implementation.

---

protiviti®