Winterhawk

SAP Access Control with Winterhawk

At Winterhawk, we have extensive experience delivering SAP Access Control to our customers with our accelerated deployment model. For more information, please contact us at info@winterhawk.com

More information on SAP Access Control can also be found here.

About Winterhawk

Winterhawk is a leading global consulting practice, supporting organisations in SAP Security, SAP GRC services and solutions (more than 20) across a variety of SAP environments including SAP R/3, S/4HANA, ARIBA, Fieldglass, Concur and SuccessFactors.

Winterhawk is the Global Solution Partner for the United VARs Alliance (Platinum SAP Partners) servicing over 8,000 clients worldwide.

united VARs
solution partner

HISTORY OF SAP SOLUTIONS: SAP ACCESS CONTROL

As part of our ongoing SAP solution spotlight series, Winterhawk spoke with Sarma Adithe, Chief Product Owner Access Governance at SAP, about the development of SAP Access Control.

What is SAP Access Control and what were its origins?

When SAP Access Control started, the primary focus was in relation to the Sarbanes Oxley (SOX) act, and it was mandatory for Segregation of Duty violations to be taken care of within organisations. This is when the Compliance Calibrator came into existence, which translated Excel spreadsheet-based analysis of violations from the existing user authorisations. When the analysis delivered a high number of violations, SAP began to think about streamlining the process; however the systems could still be contaminated if the necessary plug-ins were not implemented during the process.

At this stage, another module came in called the Risk Terminator, a service that runs in the SAP ABAP back-end system and triggers automated risk analysis checks when defined segregation of duties (SoD) access risks are violated, usually during User or Role maintenance directly in the plug-in system.

And so, SAP Access Control began to take shape; it was not just Sarbanes Oxley and a Risk Analysis tool but a streamlined access governance risk and control process. The solution has the right controls in place, which enable customers to manage the whole story in a more efficient way while fulfilling the requirements of the audit and compliance.

The next element introduced was the Access Request process, to enable end users to request access via the built-in module. Then, the Emergency Access Management came about as a means to help customers manage super access for a specific set of users for a specific time period, with all activities monitored for audit and compliance requirements. This is where Firefighter came in because SAP still wanted to address the emergency activity but within a controlled environment.

SAP then started to consolidate all the Access Risk Analysis elements within the solution, making it more business and user friendly. The process users and business process owners were involved, making it more transparent and eventually making it easier for managing compliance requirements. This is when the new Access Risk Analysis (ARA) application came in, which gives a more enhanced experience in terms of managing your roles in Risk Analysis, Batch Analysis and Adhoc analysis. Simulation at a low-level user and

introducing dashboards and reporting helped to simplify the remediation process. Then Role Management came along at a time when the landscapes were increasing and with more systems being on-boarded, it was important to have the correct controls in place.

What's new with SAP Access Control?

SAP created a remediation view which would run the analysis like a virus scanner, revealing if there are viruses present and alerting users to clean the system. SAP started to investigate at how to make it more efficient for customers to manage the process. User Access Reviews facilitate review of access and the ability to optimise it.

What the relevance for C-Suite Executives/ Insights for C-Suite Executives?

The tool started off being used for IT administration but has evolved to provide visibility of access at a level required by C-Suite Executives to ensure compliance.

SAP has also seen customers using a concept of 'zero risk' (i.e., they did not want to have any risks in their user access). This is achieved by having a very well-defined set of risks and rules to manage it. In these organisations, if any risks do pop up, they should be closely examined because their expectation is of zero risk.

Why is SAP Access Control important and what customer challenges does it address?

Access Governance is important because of the complexity of the landscape that customers operate; it's not easy to manage access across applications seamlessly. The business owners should able to focus on running their business rather having to resolve their own access which is technical in nature.

SAP knows what functions a user requires to perform their business functions, so it's a case of putting the right systems and mechanisms in place to ensure the user gets the right access. The access is managed as the user transitions or is promoted or gets additional responsibilities, while honouring the key aspects of compliance and audit, while also helping to reducing the overhead in terms of IT and avoiding potential fraud or internal threats.

What's the future of SAP Access Control?

The SAP Access Control roadmap outlines the way forward for the solution:

Recent innovations	2019 – Planned innovations[1]	2020 – Product direction[1]	2021 – Product vision[1]
Converged solution for cloud • Unified SAP Fiori launchpad • SAP Cloud Identity Access Governance bridge • Integrated role design	**Extend access governance** • Extend – SAP Ariba solutions – SAP Concur solutions – SAP Integrated Business Planning – SAP Fieldglass solutions	**Extend access governance** • Extend support to SAP Concur solutions, SAP Integrated Business Planning, and SAP Cloud for Customer	**Extend access governance to other cloud applications** • System for cross-domain identity management (SCIM)-based external applications through SAP Cloud Identity Access Governance
SAP S/4HANA support • Access risk analysis for SAP Fiori apps and OData services • Segregation of duties rule set for SAP S/4HANA, SAP Fiori apps, and OData services	**Business role management** • Business role integration with SAP Identity Management • Improved functions and features for best practices	**Business role management** • Improved functions and features for best practices	**Enhance user experience**
Emergency access management • Support for Web-based applications • Support for SAP HANA database	**Emergency access management** • Support Web-based applications **Customer connect** • Firefighter session review tracking • Mass role update of provisioning settings • Access request link to mitigation control workflow	**Access request** • Enhanced notification on access request based on actions.	**Customer feedback and enhancement requirements**
Business role management • Support for PFCG menu hierarchy for SAP Fiori catalogs		**Enhanced reporting with SAP Analytics Cloud** • Access governance data availability in SAP Analytics Cloud • Std. out-of-the-box metrics/reports • Custom reporting	**Enhance segregation of duties rule set for other applications**

There is a need for SAP to provide Access Governance for the cloud and also provide a new perspective in terms of Access Governance. SAP Cloud Identity Access Governance is a new incarnation of Access Control which is in the cloud and is a Software as a Service (SaaS) solution. It enables customers to perform Access governance for their own on-premise applications as well as their cloud applications such as HANA cloud, Ariba, Fieldglass, SAP Marketing Cloud, SAP Cloud Platform Applications and others.

SAP have also enhanced SAP Access Control with a Fiori look and feel, maintaining all the previous functionality but using the Fiori user interface.

Contact Us

Winterhawk supports clients in 90 countries. We are proud to be innovative, independent, and cost-effective. Our services are complemented with deep domain expertise, content, accelerators, and toolkits.

For further information on SAP Access Control implementation and support, or to discuss Winterhawk's Rapid Deployment Services for SAP Access Control, please get in touch with us at **info@winterhawk.com**