SOTERION: MANAGING RISK AND ENSURING COMPLIANCE THROUGH APPLICATION ACCESS MANAGEMENT

Authors:

Tom Seal
Bo Lykkegaard

March 2022

An IDC Vendor Spotlight sponsored by Soterion

IDC #EUR148915922

Soterion: Managing Risk and Ensuring Compliance Through Application Access Management

Introduction

SAP offers powerful applications that are often customized and configured to meet the evolving needs of businesses. SAP security administrators must keep pace with changing business, applications, and regulations within which the business operates.

Staying on top of SAP access rights is a challenge due to the vast number of possible access permutations and the rate at which they must be updated to keep up with organizational change. The rate of business transformation and pace of regulatory change will only increase, so organizations must find a way of preventing increased SAP access risk becoming a product of this environment.

Soterion software tackles this challenge with an access management solution that helps business users see how users utilize their access in practice and highlights the business implications of poorly configured access rights. The work that Soterion has done to convert technical access rights data into insights that business decision makers can understand and monitor continuously will help access management become proactive, rather than something to be tackled periodically ahead of an audit.

AT A GLANCE

KEY TAKEAWAYS

- SAP access management is highly complex and is difficult to maintain as business, processes, and regulations change
- Poor access management can lead to compromised processes that present a business risk and audit failures
- SAP access management is technical in nature, but access decisions are best made by risk owners and line managers
- Soterion software helps business managers understand, implement, and monitor access to SAP, reducing risk and improving efficiency

Benefits

This Vendor Spotlight explains why SAP access management is such a complex undertaking for businesses and why it is so important to get it right. We describe the increasing regulatory pressures on businesses and why this means tighter management of user access rights.

There are benefits associated with improving access management that go beyond the mitigation of risk. We explain the benefits and what is required to drive improvement. Access management tools are key to driving improvement, and in this document we profile Soterion, a provider of SAP access management solutions.

Trends

Access Control is Central to the Management of Key Business Risks

Businesses put processes in place to protect themselves from financial, reputational, and legal risks. These processes ensure that key actions have been taken, while preventing others from taking place. They reduce risk as they prevent individuals from being able to accidently or deliberately break rules set by the business or the regulators that oversee them.

In modern business, these processes are executed on digital platforms, and this enables the design of very robust processes that are excellent at protecting businesses from the array of risks they face. These processes are designed to protect the business from:

Financial Risk

Financial processes must be designed to prevent fraud by those inside the business. Segregation of duties is a key technique to protect against fraud, the principle being that transactions must always require action from two or more staff, making it extremely difficult for an individual to commit fraud and more likely user errors will be picked up.

Reputational Risk

Businesses must protect their reputation among customers and investors. The failure of risk management processes can have a big impact on the reputation of a business as well as direct financial losses or legal repercussions. In Europe, a series of corporate scandals and failures have made the public aware of the fact that not all businesses meet the standards required of them, reducing trust in the business in question. This loss of trust can have a material impact on brand value and the share price of listed companies.

Regulatory Risk

Applying processes that manage risk goes beyond good business practice. All businesses are legally required to comply with regulations determined by the jurisdictions in which they operate. Businesses in certain industries such as financial services and pharmaceuticals must adhere to a specific set of regulations driven by the types of products they develop and sell. Auditors will check compliance with these regulations. Critically, it is not enough for a business to show that no failures occurred; regulators and auditors must see that robust processes are in place to ensure continued compliance.

Privacy Risk

An example of a set of regulations that apply to all businesses in Europe are those set out in the General Data Protection Regulations (GDPR). All businesses that operate in Europe must treat personal data in line with a set of rules that control the way data is collected and consent for its use, storage, and retention is handled. There are serious penalties for organizations that breach these regulations.

Access Control

Processes designed to mitigate financial, reputational, and legal risks are the first part of the solution; access control is the second. The effectiveness of business processes is contingent on

the correct people actioning each step of the process. Risk management is ultimately in the hands of people who must perform the role defined for them precisely. Individuals with access rights to systems that are too broad may find they are able to circumvent or compromise processes designed to protect the business.

Compliance is a Complex and Evolving Challenge

The chief financial officer is the primary owner of risk management, answerable to the board, and holding a personal legal responsibility. In Europe, the regulatory burden has been rising as the European Union in particular seeks to protect consumers and investors and reduce systemic risks in certain industries. The financial crisis of 2008 in particular triggered a wave of new regulations. CFOs had to respond quickly and received investment to upgrade systems and processes to meet emerging requirements, but in most cases compliance was achieved by adjusting existing systems to meet the new requirements of regulations such as MIFID, IFRS, and SOX.

What this Means for Access Control

Organizations have modified their existing applications, including SAP, to achieve compliance. They have added new modules, reconfigured processes and used customizations in the course of developing compliant processes. Legacy applications were not designed to support current regulations, so many of these new processes have had to include compromises that create inefficiencies or poor user experience.

New processes require staff to perform differing roles, and often under stricter sets of constraints. This means a new set of access controls is required. These controls must balance the need to comply with new rules with the need for staff to perform their roles, much of which may remain unchanged.

SAP access rights themselves come with a legacy; they were often created from scratch to meet the needs of a set of roles over a decade ago. These original roles and their associated access rights were tweaked over the years to meet the needs of individuals and the changing needs of the business. New joiners typically received cloned access based on that of an individual performing a similar role. Individuals are unable to perform their roles when they have insufficient access rights, but the fact that they might have unnecessarily broad access could go unnoticed. As a result, over time a population of users emerges that has far greater system access than they truly require to perform their role.

To manage risk and ensure compliance, access management must be modernized to ensure:

- Segregation of duties: The relationship between access rights and business process must ensure that no individual can execute sensitive processes in isolation.
- Critical access: Individuals only have access to data and capabilities required for their role.
- Privacy: Staff should only see sensitive information when it is required to execute their task. Where staff can access sensitive data their ability to export the data should only be enabled when this is essential for their role.

- Organizational level control: Access should be ring fenced by geographic or organizational boundaries.

Modern applications are better designed to meet the demands of current regulations and in many cases apply design principles that should help manage any future regulatory demands. These principles include privacy by design and security by design, and the idea here is that the need to deliver privacy and security is baked into the design thinking right from the start. Application modernization, and the move to SAP S/4HANA represents a valuable opportunity to revisit access rights and avoid carrying over access risks from older systems.

SAP Access Management is Highly Complex

SAP ECC (ERP Central Component — also called SAP ERP) manages access via the transaction type (i.e., transaction codes) and user type (e.g., dialog user, service user, communication user) and allows the definition of roles that apply to one individual or a group of users. This sounds reasonable and straight-forward, but vast dimensions of typical SAP installations means that it is not:

- Over 140,000 transaction codes in SAP ECC
- Thousands of users that are not easily aggregated into roles with identical or highly similar access needs
- Often multiple legal or geographic entities with separate SAP installations and separate access management needs
- Frequent changes in access management requirements due to reorganizations, spin-offs, consolidations, changes in business scope, etc.

SAP's next-generation ERP system, S/4HANA, shifts many of the traditional business functions/ activities (e.g., the creation of a purchase order) from transaction codes in SAP GUI to Fiori applications. This enhancement has resulted in an improved, next-generation user experience. However, it has added an additional layer of complexity from a security perspective. The traditional ABAP layer manages security in the SAP GUI, but also manages the new Fiori applications, as well as linking users to the correct Fiori catalogs in SAP.

Trading off Cost and Risk

There is a balance to be found between the effort invested in access management and risk. Rigorous access management can be expensive due to the complexity of the activity, driven by the large number of staff with access and the broad range of roles they play in diverse organizations. The fast rate at which organizations, regulations, and the workforce changes also means reviewing access rights must be a frequent exercise.

The reality in many organizations is that access management is conducted annually in anticipation of, or in response to the pressures of meeting audit requirements. This reactive process then falls upon the IT function to execute, due to the technical nature of applying access changes to access rights and the way rights are documented. Access management for SAP is a highly specialized skillset that requires a deep understanding of the broad array of SAP transactions, the way these relate to the roles people hold, and the way corporate structures are reflected with SAP.

Managers will likely just confirm that staff are still employed and performing a role that requires the access rights assigned at a high level. This rolling over of access rights, without regard to changes in the business or SAP implementation, creates a disconnect between access rights and the security needs of the business.

The Cost of Poor Access Management

Poor access management is most likely to be identified during either a statutory or internal audit, as these audits set out to identify weaknesses in an organization's processes that present a risk to the organization and its various stakeholders, customers, and suppliers. The cost of poor access management extends beyond the risk of fraud and the cost of remediation. Incorrect access rights can be the root cause of an array of process inefficiencies, where users underutilize the technology available to them as they are unable to fully capitalize on it.

Where staff do not have the access rights they require, there is time taken to correct this as risk managers and line managers approve the individual's new access rights. There is also a link between access rights and software licensing and so errors in access rights can lead to under or over licensing, resulting in costs either way.

The Importance of Access Control Tool Selection

Businesses have a choice of tools they can use to manage access in SAP. The choice an organization makes should be guided by the business objectives targeted, the maturity of governance, risk, and compliance and the internal capabilities and skill sets.

Improving Access Management

To drive improvement, access management responsibilities must be shared between the IT function and the process owners and managers. Process owners are best placed to determine the rights required to execute a task within the relevant compliance rules, while managers are best placed to allocate roles to the individuals they manage. Importantly, these business owners will be able to proactively manage and maintain access rights within their domain, given the right tools. This helps move access management from an annual reactive activity towards being an exercise in continuous compliance.

Empowered business owners will be able to map processes, identify weaknesses, and implement improvements. Understanding precisely how individuals interact with SAP processes enables organizations to apply the principle of least privilege to each member of staff, reducing risk without harming productivity.

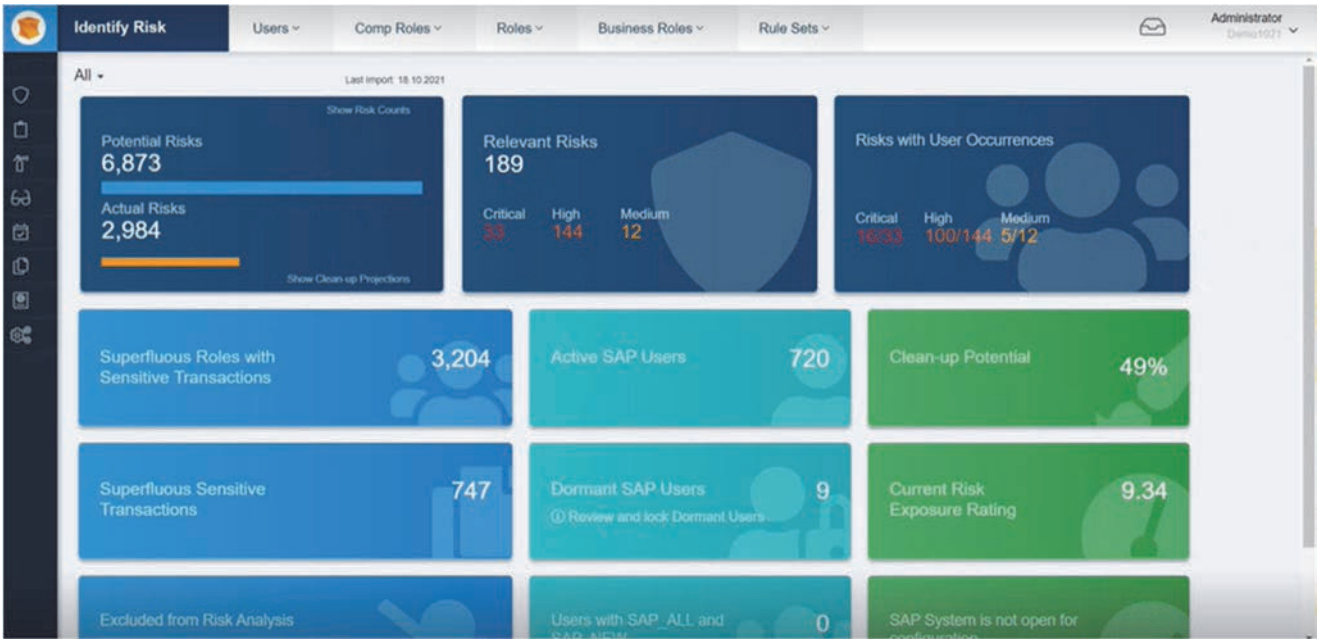
Further improvements can be achieved through the automation of access management tasks, reducing effort and improving reliability. Access revocation, for example, can be automated, reducing the chances of access being left open after a member of staff moves positions internally or leaves the organization.

Vendor Profile

Soterion is a software company focusing on governance, risk, and compliance (GRC) for SAP environments. It was founded in 2011 in South Africa by Dudley Cartwright and Johan van Noordwyk. The founders had been working on SAP access control for years and saw a need for a more agile, automated, and business-centric approach to GRC in SAP installations.

By creating Soterion for SAP as an independent, non-ABAP application, Soterion has been able to create a more modern, intuitive, and business-centric user experience, as shown on the screen shot on Figure 1.

FIGURE 1
The Soterion for SAP Overview Dashboard



Source: Soterion

The non-ABAP stack has also eased the inclusion of other solutions, such as SAP S/4HANA or other SAP SaaS applications such as Success Factors and Employee Cloud Payroll into the Soterion GRC framework. Finally, it has enabled Soterion to offer the product in multiple deployment formats, depending on customer preference:

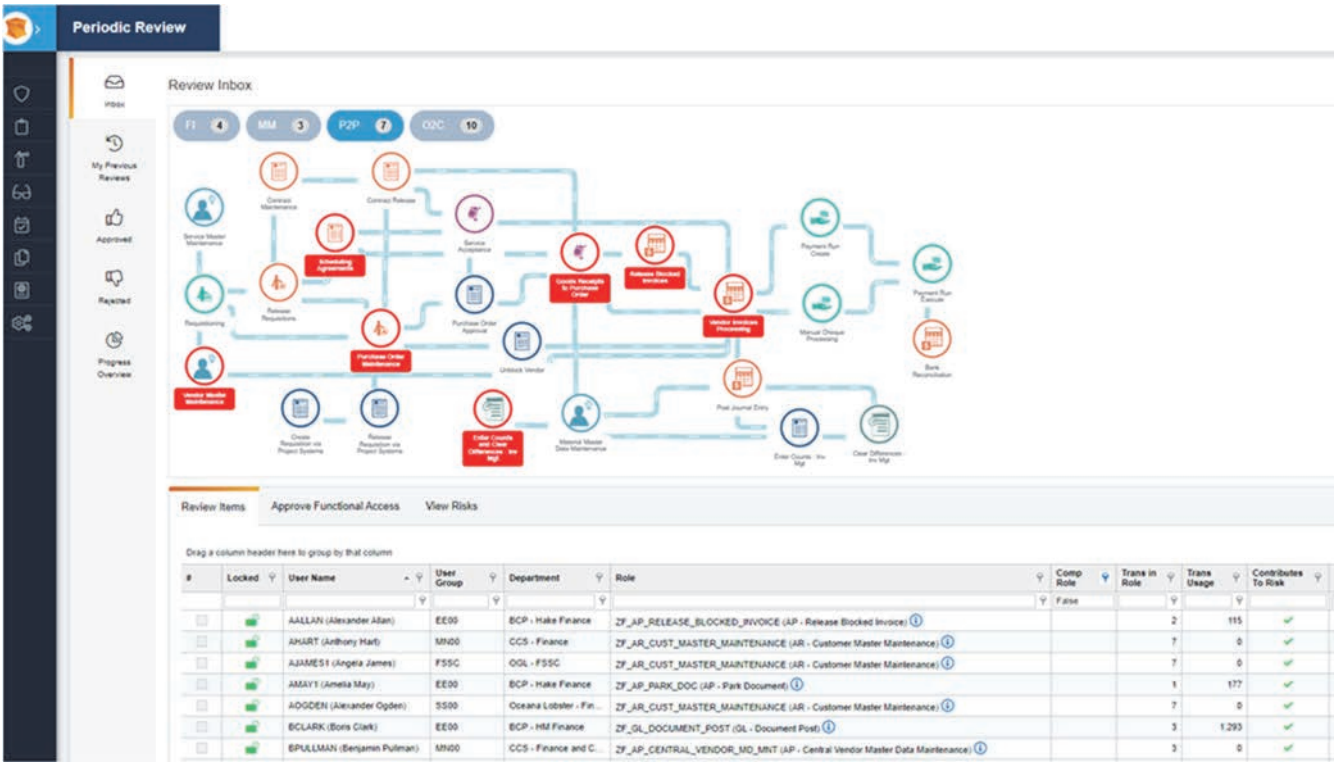
1. Software-as-a-Service (subscription based)
2. Managed service (custom subscription)
3. On-premises (license and maintenance based)

Soterion for SAP features the same user experience across deployment formats and across modules. The main module is the Access Risk Manager, which provides insights into current access risks in the SAP environment. The Access Risk Manager offers functionality to reduce access risks, keep access risks low, analyze privacy implications, etc. A key differentiator of Soterion is its reporting capabilities, which illustrates access risks in business process flow diagrams (Figure 2). For business users that are not SAP transaction code experts, it simplifies

understanding where in the business process the conflicting access resides. By converting the technical GRC language into a language the business users can understand, this can help in making better decisions and making business users more involved and accountable in the process. Ultimately, this can improve the overall capability of the organization to manage its risk.

FIGURE 2

Business Process Flow Diagrams Helps Line Managers to Identify Where in the Business Process Access Resides



Source: Soterion

Another key module is the SAP Basis Review, which involves user checks for critical configuration such as production users with developer keys or test users working in production environments. The Elevated Rights Manager enables managing elevated entitlements and mitigating associated risks. This process includes identifying and mapping users that have elevated rights access, checking their level of access, and monitoring emergency activities performed by such users. Finally, the solution has modules such as Periodic Review Manager, SAP Licensing Manager, Data Privacy Manager, and Central Identity Manager.

Future Roadmap for Soterion

The company is evolving its business in several directions. Firstly, it is expanding its access control and broader GRC footprint to other SAP SaaS solutions (e.g., Ariba, Concur) and to non-SAP solutions that are used by many SAP customers (e.g., Salesforce.com and Coupa). This will enable customers to perform access and risk profiling, grouping, and reporting across applications.

Secondly, Soterion is planning to move into the identity management space via packaged integration with key vendors in this space. Combining access control and user/identity management in an integrated console will ease administrative tasks.

Thirdly, Soterion is planning to add a third risk level (materialized risk) to the current two risk levels (potential risk and actual risk). Potential risk includes all cases where a user has the potential to violate segregation of duties. Actual risk includes all cases where a user has actually used both conflicting transaction codes in SAP (e.g., create/edit purchase order and release purchase order). Materialized risk includes cases where the conflicting transaction codes have been used on the same item, such as editing and releasing the same purchase order.

Finally, Soterion plans to release a Compliance Manager solution, which will be based on the experience gathered being a managed service provider. Many compliance managers have common requirements in terms of the KPIs they want to track, the workflows they want automated, and the reporting that they need.

Challenges

- **Play into larger identity and access management propositions.** As customers are increasingly looking for pre-integration solution sets to shorten implementation time and get faster time-to-value, Soterion must increase collaborations with other vendors in this space to offer out-of-the-box integration. This will significantly help in getting shortlisted and winning future deals. Currently, Soterion is looking into pre-integration with ServiceNow and OneTrust, as well as extending its own solution footprint further.
- **Soterion must expand geographically to gain scale in a global SAP ERP market.** Its expertise in business-centric SAP access control is applicable across SAP geographies. Soterion currently has representatives in countries such as the U.K., Netherlands, and Australia. However, considering the large SAP installed bases in Germany, the U.S., the Nordics, France, China, and so on, IDC sees significant potential for geographical expansion.
- **Increasingly target the CFO and line of business decision makers** in addition to the SAP expertise center and IT function. IDC foresees that both the buying power and the impetus to improve access management risks will reside with the CFO rather than IT. This will require Soterion to focus future value propositions on CFOs. In concrete terms, the key selling points must focus more on administrative efficiency (for finance and IT professionals) and better risk mitigation related to internal fraud and privacy breaches and less on IT-related features and functions in the access management space.

Future Outlook

- **Artificial intelligence (AI)** takes center stage to reduce access control complexity. Current access management solutions are mainly based on programmed logic and fixed algorithms checking for known segregation of duty conflicts, etc. Future solutions will use machine learning to identify and suggest possible remedies to overprovisioning of user rights and identify actual segregation of duty risks.

- **Access and identity management consolidation.** Customers are increasingly unwilling to integrate access and identity solutions from multiple vendors themselves. Consequently, access and identity management vendors will consolidate solutions via both acquisitions and APIs. Furthermore, IDC expects vendors to continue to develop in those areas where they have gaps. As an example, Soterion is developing identity management capabilities and a number of identity management vendors are developing access risk capabilities. Some customers will prefer a best of breed approach, particularly those with high emphasis on risk, while others will prefer broader identity management suites, particularly those looking for process efficiencies.
- **Future CFO agenda requires new automation levels, including in compliance management.** The finance department of the future is highly IT-driven and automated. Focus will be on higher value tasks such as advisory and planning, facilitation of self-service reporting, and supporting business initiatives. Ensuring segregation of duties compliance, licensing compliance, and keeping access controls up to date are clear candidates for automation. Without automation, IT and finance departments will be faced with the hard choice of either spending excessive efforts on manual access control management or to over-allow users and thereby ignore the resulting business risks and costs of over-licensing.

Conclusion

Managing SAP access rights is highly complex due to the vast array of process and role configurations that organizations can and do utilize within their SAP applications. As organizations evolve and adopt new applications, the burden of managing access rights only increases, leading to increased costs and risks, particularly the chance of audits identifying control weaknesses resulting from SAP access irregularities.

SAP access must be managed proactively, and to do this a tool is required to monitor, interpret, and optimize each user's access as it pertains to their role. Soterion provides such a tool, and a key differentiator is that it has been developed with the business user in mind. Decisions regarding SAP access are best made by those that understand the business context in which processes and the staff who interact with them operate. Soterion's tool helps visualize the relationship between access rights and business processes, highlighting weaknesses in a way that managers can quickly comprehend. The power of this tool is that it puts control in the hands of those best placed to make decisions.

Soterion is now expanding the capabilities of its product to address a broader array of governance, risk, and compliance (GRC) challenges. This will help Soterion support the CFO as they tackle the major challenge of operating within an increasingly broad and diverse regulatory landscape.

MESSAGE FROM THE SPONSOR

Soterion is an international leading provider of governance, risk, and compliance solutions for organizations running SAP. Soterion's user-friendly GRC solutions provide in-depth access risk reporting to allow organizations to effectively manage their access risk exposure. Soterion is passionate about simplifying the governance, risk, and compliance processes, with a focus on translating this complexity into a business-friendly language to enhance better decision making and business accountability.

Email info@soterion.com for more information.

About the Analysts

Tom Seal, Senior Research Director, European Enterprise Applications

Tom Seal is a senior research director in IDC's European enterprise applications team. He has over 20 years' experience as an analyst, consultant, and technology procurement manager. He focuses on the ERP market and the future of the finance and procurement functions. Current research includes investigating the business case for ERP modernization and the economics of cloud technology.

Bo Lykkegaard, Associate VP for the Software Tracker, Public Cloud Services Tracker, and European Enterprise Applications Research

Bo Lykkegaard is associate vice president for the enterprise-software-related expertise centers in Europe and the quantitative software research team in Europe. His team focuses on the $172 billion European software market, specifically on business applications, customer experience, business analytics, and artificial intelligence. Specific research areas include market analysis, competitive analysis, end-user case studies and surveys, thought leadership, and custom market models.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

Copyright and Restrictions