September 2019

Soterion

Innovation in User Experience for Automated Controls

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

Monitoring and Managing Access Controls 4
- Efficiency Required in Access Control & Segregation of Duties 4
- Understanding the Interrelationship of Access Controls 5

Soterion 6
- Innovation in User Experience for Automated Controls 6
- What Soterion Does 8
- Benefits Organizations Have Received with Soterion 10
- Considerations in Context of Soterion 11

About GRC 20/20 Research, LLC 13

Research Methodology 13

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

Soterion

Innovation in User Experience for Automated Controls

Monitoring and Managing Access Controls

Efficiency Required in Access Control & Segregation of Duties

Business is impacted by constant change. Change is the single greatest governance, risk management, and compliance (GRC) challenge today. Today's organization is in a continuous state of change with shifting employees: new ones are hired, others change roles, while others leave or are terminated. Business processes and technology change at a rapid pace. In the context of change, internal controls over financial reporting, regulatory requirements (e.g., SOX), internal and external auditors, and fraud risk put increased pressure on corporations to ensure all ERP and critical business systems are secure and access control risks are managed across a dynamic and distributed business environment. Organizations often fail to monitor and manage access controls efficiently and effectively in an environment that demands agility. Too often access control management is a periodic exercise that provides incomplete visibility into the organization's people, processes, and business systems.

Gone are the years of simplicity in business operations. Exponential growth and change in risks, regulations, globalization, employees, distributed operations, competitive velocity, technology, and business data encumbers organizations of all sizes. Keeping risk, complexity, and change in sync is a significant challenge throughout all levels of the business. This challenge is greater when access control management and automation is done in manual processes or silos and is not an ongoing and monitored process within ERP applications, such as SAP. Organizations need to understand how to design effective access controls, implement them, and review whether the risks they were designed to control are effectively mitigated on a continuous and ongoing basis.

Corporate governance and organizational culture have largely been based on trust. In this context the organization trusts their employees, contractors, and other parties working on its behalf. It is understood that these individuals will follow policies and procedures. The reality is that people are human. They make mistakes, they cut corners, and their own motives and goals may not align with the organizations. This is further confounded when management undermines controls they find bothersome. Keeping up with controls in a changing workforce environment with access to ERP systems as regulations, risks, applications, priorities, and business processes change is challenging. There is a need to automate the access controls to bring real-time insight into what individuals are actually doing in ERP environments to mitigate user access and process risks.

Understanding the Interrelationship of Access Controls

Access control management and automation is often misunderstood, misapplied, and misinterpreted as a result of scattered and uncoordinated approaches. This is particularly true when access controls are a set of manual processes encumbered by documents, spreadsheets, and emails when it could be continuously monitored and enforced in the ERP environment. Managing segregation of duties (SoD), inherited rights, critical and super user access, and changes to roles in manual processes is a losing battle.

The management of access controls has become increasingly challenging as the organization has:

- ***Multiple lines of businesses operating globally*** across many jurisdictions and systems.
- ***Workforce that is constantly changing*** with access into systems and processes. Over time there are significant gaps and access rights issues.
- ***Web of third-party relationships*** of contractors, consultants, temporary workers, service providers, and outsourcers that have access to data, systems, and processes.
- ***Mergers and acquisitions that exponentially grows*** the systems, processes, and controls in the organization if not properly integrated.
- ***Millions of dollars in transactions*** that flow through business systems in the digital economy that need controls.

Manual processes and document-centric approaches to SoD, inherited rights, and critical/super user access is time-consuming, prone to mistakes and errors, and leave the business exposed. Completing a control assessment process and ticking the box has got in the way of true access control analysis and understanding. Documents and spreadsheets are not equipped to capture the complex interrelationships that span systems, operations, transactions, lines of business, and processes. Surprisingly, many organizations still use these manual processes to manage access control and SoD risk. Not only are these approaches inefficient and ineffective, slowing the business down, but they introduce greater exposure to risk and non-compliance, as it is nearly impossible to keep up with the pace of change in employees and access in ERP systems.

The inefficient, ineffective, and non-agile organization runs a combination of security and access reports, and compiles access information into documents and spreadsheets that are sent out via email (used as an improvised workflow tool) for review and analysis. At the end of the day, significant time is spent running reports, compiling and integrating that information into documents and spreadsheets to send out for review. This ends up costing the organization in wasted resources, errors in manual reporting, and audit time drilling into configurations and testing access controls in the ERP environment. Organizations often miss things, as there is no structure of accountability with audit trails. This approach is not scalable and becomes unmanageable over time. It leads to

a false sense of control due to reliance on inaccurate and misleading results from errors produced by manual access control processes.

By automating access controls, organizations take a proactive approach to avoiding risk while cutting down the cost and time required to maintain controls, be compliant, and mitigate risk. The organization must have holistic visibility and 360° contextual awareness into access control and risk relationships. Complexity of business and intricacy, and interconnectedness of control data, requires that the organization implement an enterprise view of access controls.

The bottom line: Technology for access control management, automation, and continuous monitoring now enable organizations to achieve a real-time, integrated view of enterprise access controls and risks. This not only enables an enterprise perspective of access risk, but also allows the organization to increase efficiency, effectiveness, and agility in access control management and automation. To address access control risk, organizations are establishing an access control and SoD strategy with process and technology to build and maintain an access control program that balances business agility, control, and security to mitigate risk, reduce loss/exposure, and satisfy auditors and regulators - while enabling users to perform their jobs. When evaluating solutions for SoD and access controls the organization needs solutions that are intuitive and easy to use.

Soterion

Innovation in User Experience for Automated Controls

Soterion is a solution that GRC 20/20 has researched, evaluated, and reviewed with organizations that are using it in complex, distributed, and dynamic business environments. Soterion is an agile access and automated control platform for SAP environments with capabilities to manage access controls in an easy-to-use and intuitive environment that delivers significant business value and brings a contextual understanding of access management that is relevant to a business user. In this context, GRC 20/20 is recognizing Soterion with a ***2019 GRC User Experience Award in Automated and Continuous Control Monitoring.***

Soterion was established in 2011 with a defined focus in SAP Access Security and Risk. They have worked with organizations across multiple industries, geographies, and sizes with a highly agile and intuitive solution that fits a range of cultures and approaches. This solution is offered in both a subscription as well as a perpetual license format and can be delivered in the following ways:

- **Soterion On-Premise.** This is for customers that want the solution installed within their own data centers on their own servers.
- **Soterion Cloud.** This is for customers that want Soterion to host the solution in Soterion's Cloud infrastructure and servers.

- **Soterion GRC as a Managed Service.** This is for customers that want to leverage both Soterion's technology, as well as expertise in monitoring SAP access management.

GRC 20/20 finds the Soterion solution to be easy to use and intuitive for the business user, as well as the GRC professional. This makes it an ideal solution that manages SAP access management and risk from the front office to the back office of GRC that crosses all three lines of defense. It is cost-effective and agile for small organizations to large organizations.

Some of the key differentiators that GRC 20/20 has noted in the Soterion solution is its ability to do business process modeling to define access rights in the context of business process flows and diagramming, understanding access risk in a business user context, and detailed privacy access risk functionality (e.g., GDPR, CCPA) to manage access to personal information in a privacy context.

GRC 20/20's evaluation, research, and interactions with Soterion clients has determined the following:

- **Before Soterion:** Clients of Soterion typically are replacing manual processes of SAP access management that are encumbered by documents, spreadsheets, and emails. Such approaches can be very time-consuming, and prone to errors - particularly in aggregation and reporting on access data that involves hundreds to thousands of documents and spreadsheets. Other customers worked with other SAP access management solutions and found them to be too complex and costly to own and moved to Soterion for its ease of use and lower cost of ownership.

- **Why Soterion:** Organizations choose Soterion as they are looking for an intuitive SAP access risk management solution that is easy to use by the business. Clients state they chose Soterion as the flexibility, acquisition cost, rapid implementation, and ongoing ownership/maintenance costs were more affordable than the competition, and it is easy to maintain and configure to their environments. They saw the opportunity with Soterion - to move from reactive access management firefighting to proactive SAP access management planning and risk management.

- **How Soterion is used:** Typical use cases for Soterion in SAP environments include:

  - SAP user access risk management and reviews
  - Role mining
  - Segregation of duty rulesets
  - Fire fighter access to consultants and support staff

- Ensuring standard audit requirements for access and security settings in SAP
- Access risk validation modeling before implementation of changes

- **Where Soterion has excelled:** Organizations consistently state that Soterion has improved the quality and reporting of their SAP access risk management related processes and information. This improves the organization's overall visibility into SAP access risks in context of the organization's processes and information (e.g., such as access to EU citizen data in a GDPR context), while eliminating the overhead of managing manual processes encumbered by hundreds to thousands of spreadsheets, documents, and emails. Clients find that the solution is flexible to adapt to their organization's access risk management requirements, has the core capabilities needed, and provides them the ability to grow and mature their program over time. Overall, users find the solution adaptable and agile to meet diverse access risk management process requirements. Some of the comments GRC 20/20 has collected from Soterion clients include:
  - *"The system gives us a solid base to ensure we have the required controls over access, and it provides detail reporting on access that when we need to investigate, we have the required reports available."*
  - *"The biggest benefit is that our auditors have confidence in the system, and we therefore can justify that the conflicts we have can be mitigated, and therefore we can keep our head count in check."*
  - *"In ensuring that we are compliant with our internal audit – this was an area that we were never compliant on. Also enable us to get buy-in and ownership from business."*
  - *"It's easy to use and instead of saying you can't have access to role A and B together, it also has a short description of the conflicts. Their support team is also fantastic. They're always very helpful."*

What Soterion Does

In today's environment, organizations are required to create and maintain access risk in complex ERP environments. This is challenging in the context of continuous business change such as new employees, as well as employees that change roles and introduce inherited rights issues leading to further segregation of duty issues. Mergers and acquisitions bring in redundant ERP environments and more users and potential risks and conflicts. Many organizations across large and mid-sized enterprises find their SAP access risk management tasks tedious and time-consuming because they lack data analysis and reporting features due to of manual document-centric processes. They desire the ability to access reports, dashboards, and underlying access risk data in real time. GRC managers and experts find it difficult to cope with the rapid evolution of the business and related SAP access and configuration changes, while ensuring the ongoing monitoring and enforcement of access controls.

The Soterion for SAP access risk management suite of solutions includes:

- **Access Risk Manager.** This solution enables the organization to understand, simulate, and mitigate risk in SAP authorizations and access.
  - *Identify Risk Module* examines SAP user authorizations in the context of the user's historical transactions. The module specifically looks at segregation of duties, critical transactions, and privacy risk. This enables the organization to not only identify potential access risks, but also recognize and monitor actual access risk.
  - *Get Clean Module* analyzes SAP access risk by conducting a gap analysis between the potential SAP access risk and the actual SAP access risk. Through the use of clean-up wizards, the organization can get clear guidance on how to reduce or eliminate access risk. Suggestions are made in context of removal of unnecessary access rights/allocations, as well as the splitting of roles based on role usage.
  - *Stay Clean Module* provides for the simulation of 'what-if' SAP authorization and access right changes before they are implemented in the real-world SAP environment. It leverages user transactional history in simulations to understand what the risk changes can bring to the organization. There is standardized workflow and tasks to manage authorization and access changes with the business who owns the risk.
  - *Stay in Control Module* automates the application of mitigating controls for access risk. This is enabled through standardized rule sets provided in Soterion, and detailed workflow to the business to approve authorizations and changes.
- **Basis Review Manager.** This solution allows for the ongoing auditing and monitoring of an organization's SAP basis configuration against a set of industry standard best practices. These practices can be customized to the organization's specific requirements.
- **Elevated Rights Manager.** This solution allows the organization to grant and monitor elevated (e.g., super user) access to approved users for a limited time. It provides robust audit trails of activities performed to ensure nothing unauthorized or unwanted occurred.
- **Periodic Review Manager.** This solution automates with workflow, tasks, and reporting the periodic review, approvals, and changes to access needed by the business. Reports are delivered that includes risk context and actual role usage through transactional data.
- **Employee Self Service.** This solution allows users to request access in the SAP environment. This can be at the individual level, or for managers to request

access for their employees. Workflow is set up that provides access risk and history for approvers to see the request in context.

- **SAP License Manager.** This solution monitors the actual use of SAP licenses to ensure that users are correctly classified, and that SAP agreements are correct to reflect actual usage and licensing requirements.

Soterion delivers an intuitive, easy to use, robust, and future-ready SAP access risk management platform that simplifies and strengthens regulatory compliance and risk management in line with industry standards and best practices, while focusing on the end user's ease of use and GRC administrator's ease of change. GRC 20/20 has evaluated the features and capabilities of Soterion and finds that it delivers an agile, intuitive, and engaging solution for enterprise SAP access management. Soterion is an innovative, intuitive platform that modernizes how people work and interact with SAP access processes across the enterprise. It is used to collect, organize, link, report, and analyze access risk data with increased control, collaboration, transparency, and accountability.

Benefits Organizations Have Received with Soterion

Most Soterion clients moved to the solution because they found their manual document-centric approaches for SAP access management consumed too many resources. Too often things were getting missed in the continuous barrage of SAP access complexity, as well as in regulatory and business change. Others moved to Soterion as they found their previous SAP access risk solution was dated, cumbersome, too costly to own and maintain, and lacked the ease-of-use and intuitiveness that the business needed to understand SAP access risk and related processes. Across these clients, there is consistent praise for the value of the ongoing cost of ownership of the Soterion platform, in the speed of deployment, return on investment, improved effectiveness, and agility to manage, monitor, and enforce SAP access risk.

Specific benefits that GRC 20/20 finds that Soterion clients have achieved in their implementations are:

- *360° visibility into SAP access risk* where all information is in one place and gives complete situational and contextual awareness of user access risk and history of usage in relation to business role(s).

- *Elimination of hundreds to thousands of documents, spreadsheets, and emails,* and the time needed to monitor, gather, and report on them to manage SAP access related activities and processes.

- *Significant efficiencies in time through automation* of workflow and tasks as well as reporting. Specifically, the time it took to build reports from hundreds to thousands of documents and spreadsheets now is just a matter of seconds.

- *Fewer things slipping through cracks* as there are established tasks, monitoring, notifications, and escalation when access risk exposes itself in the SAP environment.

- *Efficiency in streamlining processes* through identification of controls, access rules, requirements, accountability, tracking, and getting things done.
- *Greater granularity and ability to report* on specific SAP access risk and control details that could not be done in documents or spreadsheets.
- *Increased awareness and accountability of SAP access* by business owners who are informed on the subject matter in context of their role.
- *Collaboration and synergies across SAP access management* functions and business owners, instead of different roles doing similar things in different formats and processes.
- *Consistency and accuracy of information* as the organization conforms to consistent processes and information structures.
- *Accountability with full audit trails* of who did what and when in the SAP access environment.
- *Reduction in time needed to govern and manage SAP access requests* that are freed from manual processes - these resources can then focus on value-added activities.
- *Increased agility in context of change* that enables the organization to be proactive in keeping up with SAP access and roles when the business changes, and not just reactive - leading to less access risk exposure and being caught off-guard.
- *Mitigation of fraud in the environment* in which one Soterion customer said it was reduced 'drastically.'

Considerations in Context of Soterion

Every solution has its strengths and weaknesses and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of Soterion to enable organizations to achieve consistent SAP access risk management processes, readers should not see this as a complete and unquestionable endorsement of Soterion.

Soterion's clients praise the company for its solution delivery, but also praise it for the depth of its understanding of the SAP environment and access risk. Soterion is there to work with the client and be a true partner and knowledge source, and not just a software provider. Soterion's suite of solutions enable organizations to efficiently manage SAP access risk across complex and distributed SAP environments. The applications facilitate real-time collaboration and access risk information sharing across the enterprise and provide comprehensive visibility into access risk management and compliance.

At the end of the day, Soterion save organizations time over manual processes for SAP access risk that also delivers greater effectiveness and agility to the organization. This enables organizations to meet audit requirements, better understand segregation of duties, and document mitigating controls. Documentation and reports are ready to present to auditors and risk/board committees. Overall, it gives an organization a clear understanding of their SAP access risk that are throughout the business and does so in a context the business can understand without the overwhelming complexity IT often presents.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com