September 2015

CSI tools

A Fresh Perspective on Access Controls & SoD

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

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.

CSI tools

A Fresh Perspective on Access Controls & SoD

Struggling to Keep Up in Access Controls & SoD

Business is all about change. Change is the single greatest GRC challenge today. Organizations do not operate in a static environment that slowly evolves; today's organization is in a continuous state of change. Consider employees in context of their access to critical business systems: new ones are hired, others change roles, and still others leave or are terminated. 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 ERP systems are secure and access control risks are managed in the context of a dynamic business environment.

Change and access to internal systems is not just with traditional employees, but also with business partner relationships, such as vendors, contractors, outsourcers, service providers, and temporary workers – all of whom may have access to internal systems. However, access control is not just about risk and compliance; it is also about consistent operations. The organization needs distributed responsibilities and processes that are reliable and behave consistently. Agile access control monitoring and enforcement deliver a structured system of access governance that enables processes to work as intended without anyone maliciously or inadvertently causing an issue.

Surprisingly, many organizations still use manual processes and documents to manage access and the associated risk upon the organization. This is primarily done by spreadsheets, word processing documents, and email. The inefficient, ineffective, and non-agile organization runs a combination of ERP security and access reports, and then compiles access information into documents and spreadsheets that are sent out via email as an improvised workflow tool for review and analysis. 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 change and risk exposure that change brings.

At the end of the day, significant time is spent running reports, compiling information, and integrating that information into documents and spreadsheets to send out via e-mail for review. This manual and document-centric process ends up costing organizations significantly more in wasted resources, errors in manual reporting, and audit time drilling into the process than an automated solution costs. Worse, organizations often miss things as there is no structure of accountability and workflow and audit trails do not exist. This approach is not scalable and becomes unmanageable over time. It leads to a false sense of security due to reliance on inaccurate and misleading results from errors produced by manual processes.

This challenge grows when you consider the complex interrelationship of different ERP instances and access to those across the business environment. To reconcile access across different systems and see the big picture of access risk becomes complicated as the ERP environment grows. While organizations struggle to manage access risk within one instance of ERP, managing access across multiple ERP systems causes an exponential growth in time and resources when done by a manual and document-centric approach. In a heterogeneous environment, these challenges only become more complicated.

This means that organizations cannot rely on manual, ad hoc, and document-centric approaches to manage access to critical business systems. The issues of SoD, inherited rights, critical and super user access, compliance, risk management, and general change to roles and access is too much for today's organization to manage adequately in spreadsheets and e-mail. Growing exposure to risk and increasing regulations compound this as they require greater oversight of access to critical systems with audit validations of access control and SoD. By automating access management and SoD controls and embedding risk analysis and mitigation into user and role maintenance, organizations take a proactive approach to avoiding risk while cutting down the cost and time required to maintain compliance.

The bottom line: Manual processes and document-centric approaches to SoD, inherited rights, critical and super user access, is time-consuming, prone to mistakes and errors, and leave the business exposed. Organizations need to establish an access control and SoD strategy and process that is supported by technology to manage access control in a context that balances business agility with control and security to mitigate risk, reduce loss/exposure, and satisfy both auditors and regulators while enabling users to perform their jobs. 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.

CSI tools

A Fresh Perspective on Access Control & SoD

CSI tools is a GRC offering that GRC 20/20 has researched, evaluated, and reviewed with organizations that are using it in changing, distributed, and dynamic business environments. CSI tools provides analytic control solutions that audit and monitor SAP environments, manage and validate authorizations, and build roles tuned to the organizations security requirements and business needs. CSI tools enables organizations to evaluate existing roles, access rights of users, remediate issues, restructure roles to remove unnecessary roles and entitlements, as well as grant and document exceptions for non-compliant access for business reasons. GRC 20/20 has interviewed and engaged several CSI Tool clients and finds that the CSI tools solutions have helped them keep up with access controls and SoD in a way that maximizes their GRC resource efficiency, effectiveness, and agility.

It has been stated that:

> *Any intelligent fool can make things bigger, more complex and more violent. It takes a touch of genius – and a lot of courage to move in the opposite direction.*[1]

While there are many automated access control and SoD solutions available in the market, CSI tools takes a unique and very effective approach. CSI tools accomplishes this by focusing on authorization objects and not simply on transaction codes that other solutions do. Consider that there are roughly 150,000 transaction codes in nested relationships and complexity within SAP environments while there are only approximately 1,200 authorization objects. The exponential impact of access control and SoD around transaction codes produces millions of combinations. Transaction codes provide a rough first line of defense that can be bypassed given the right circumstances, while authorizations objects are what actually manage access rights in the SAP environment. Authorizations assigned to an SAP user give the user permission to access data independent of the user's capability to execute a transaction. While both transaction codes and authorization objects can be used to secure SAP environments, focusing on authorization objects instead of transaction codes is more effective, efficient, and agile.

Some of the capabilities that GRC 20/20 has evaluated in CSI tools that many of its competitors do not always address are:

- ✓ Which roles cause accumulation of access rights
- ✓ Who has almost access to do something
- ✓ Which roles need to be removed
- ✓ Which roles should be isolated from a composite one
- ✓ Check the access of a role based on documentation

The Value of CSI tools

Successful GRC delivers the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment with agility. GRC solutions should achieve better performing processes that utilize more reliable information. This enables a better performing, less costly, and more flexible business environment. Clients engage CSI tools with the goals of understanding and managing risk, ensuring compliance with obligations, improving human and financial efficiencies, enhancing transparency, and managing GRC in the context of business change.

GRC 20/20 measures the value of GRC engagement around the elements of efficiency, effectiveness, and agility. Organizations need to be:

1 *This quote has been attributed both to Einstein and E.F. Schumacher.*

- **Efficient.** GRC engagement provides efficiency and savings in both human and financial capital. GRC efficiency is achieved when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations.

- **Effective.** At the end of the day it is about effectiveness. How does the organization ensure risk and compliance is effectively understood, monitored, and managed at all levels of the organization?

- **Agile.** GRC engagement delivers business agility where organizations can respond rapidly to changes in the business environment (e.g., employees, business relationships, mergers, acquisitions, new laws, and regulations) and communicate to employees GRC context to these changes.

GRC Efficiency

GRC solutions provide efficiency and savings in human and financial capital resources. Technology solutions that support business and GRC processes reduce operational costs by automating processes, particularly those that take a lot of time consolidating and reconciling information in order to manage and mitigate risk and meet compliance requirements. GRC efficiency is achieved when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations. Their ability to focus on authorization objects and not just transaction codes is more effective, efficient, and agile.

The organizations researched by GRC 20/20 identified the following efficiencies by organizations using CSI tools:

- ✓ Cost savings in employee time designing user roles in context of ERP changes
- ✓ Automation of access controls and SoD brings efficiency in employee time
- ✓ Less spending on external consultants to do manual control validation and SoD monitoring
- ✓ Cost savings in internal audit testing and investigation of access controls
- ✓ Reduction in external audit fees as they rely more on the automation of access controls and SoD
- ✓ Efficiency in assigning and determining appropriate access
- ✓ Greater efficiency and savings in resource time documenting user access reviews
- ✓ Efficiency in technology processing and overall reporting time savings in which an audit of 10,000 users takes only 15 minutes

GRC Effectiveness

GRC solutions achieve effectiveness in risk, control, compliance, audit, and business processes. This is delivered through greater assurance of the design and operational effectiveness of controls to mitigate risk, achieve performance, protect integrity of the organization, and meet regulatory requirements. GRC effectiveness is validated when business processes are operating within the controls and policies set by the organization and provide greater reliability of information to auditors and regulators.

The organizations GRC 20/20 interviewed reported the following effectiveness through utilizing CSI tools:

- ✓ Access provisioning, monitoring, SoD, and emergency management are now practical through automation as the organization never had the time and resources to properly address these manually
- ✓ The organization now audits all roles for SoD issues instead of random sampling
- ✓ Reduction in auditor findings related to SoD conflicts
- ✓ Reduction in risk exposure as well as business disruption through stronger control enforcement and monitoring
- ✓ Performing authorization reviews manually was like "looking for a needle in a haystack" but is now practical and effective with a greater number of SoD conflicts detected and addressed
- ✓ Easy to determine users with excessive access, who have SoD conflicts, determine the roles that are causing conflicts or excessive access
- ✓ Ability to customize queries to solve specific authorization challenges
- ✓ Reduction of 32,000 SoD conflicts to 4,000 in the first month of use

GRC Agility

GRC solutions deliver business agility where organizations are able to rapidly respond to changes in the internal business environment (e.g., employees, business relationships, operational risks, mergers, and acquisitions) as well as the external environment (e.g., economic risk, new laws, and regulations). GRC agility is also achieved when organizations can identify and react quickly to control failures/weaknesses, non-compliance, and adverse events in a timely manner so that action can be taken.

The organizations interviewed reported the following agilities in their compliance and broader GRC processes through working with CSI tools:

- ✓ The organization is now able to rapidly find and correct access control and SoD issues

- ✓ Once queries are built and customized they can be readily used at any time
- ✓ Authorizations are more transparent
- ✓ Capability to present conflicting roles to the business in a way they can understand and respond to
- ✓ Ability to manage action items to fix authorization problems
- ✓ Streamlined authorization audits and consultations
- ✓ Ability to continuously monitor role and SoD changes throughout year and not just annually

Capabilities of CSI tools

GRC 20/20 has evaluated the CSI tools offering and finds that it delivers an integrated and harmonized solution for today's demanding access control and SoD challenges faced by organizations across industries and geographies. CSI tools enables organizations to evaluate the existing roles and access rights of users, remediate issues, restructure roles to remove unnecessary roles and entitlements, as well as grant and document exceptions for non-compliant access for business reasons.

CSI tools delivers the following capabilities to make GRC programs efficient, effective, and agile:

- **Rule-Based SoD analysis.** Analysis of SoD is built on an extensive set of authorization object analysis that can be built into rules that meet specific business needs and scenarios. SAP has multi-layered security. Other solutions check layers simultaneously to ensure that there are no false positives. CSI tools does five independent checks. By analyzing different layers separately organizations can identify conceptual weaknesses in the roles as well as weaknesses in rules.
- **Compliant access provisioning.** CSI tools enables compliant access provisioning with workflow for access request, policy analysis, approvals, and access fulfillment.
- **Transaction and role analysis.** CSI tools uses the executed transaction information to report if SoD conflicts or critical functionality in SAP systems have been executed by users (together with the frequency of usage and last date it was used). This executed transaction information is used to maintain and build roles.
- **Emergency access management.** CSI tools allows for emergency access management and monitoring of emergency access given in those situations that the organization needs to react and do something quickly.

- **Role management and design.** CSI tools has advanced functionality to help organizations design and mange roles in the SAP environment and to streamline role redesign based on SoD conflicts and role usage. Roles can even be built automatically through the use of CSI tools. CSI tools provides a complete solution to define SAP roles and assignments and is used to build composite roles.

- **Access certification.** CSI tools provides a streamlined ability to manage access certification to ensure that the organizations users are given the access rights they need and no more.

- **Reporting & dashboards.** CSI tools has advanced reporting capabilities that allows organizations to customize queries and reports to their specific scenarios and needs.

- **Access remediation.** CSI tools enables the process of remediation upon determining there is a conflict through analysis of how access is being given and used and defining remediation tasks to be taken. CSI tools provides answers to questions like: Is the access appropriate? How is the user getting access to these conflicts? Is the user really using this critical functionality and by which roles?

- **License manager.** CSI tools has a license manager to simulate how SAP licenses will be used given role redesign. The license manager analyzes if the correct SAP licenses are assigned in the SAP system that delivers insights if users and roles are assigned to the correct SAP license. This makes it also possible to simulate how much organizations can save if access rights are reduced.

- **Controls organizer.** CSI tools documents risks and controls throughout business processes and sub-processes. Control measures like compensating controls can be assigned to mitigate risks and by which configuration controls of SAP settings can be checked automatically. All monitoring and audit evidence is stored.

- **Quality assurance.** CSI tools has integrated checks to make sure roles are defined and built correctly.

- **Codification.** CSI tools defines the hierarchical structure on the what and where. Both organizational and non-organizational values can be documented centrally to automate role derivation.

Considerations for CSI tools

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 CSI tools to enable GRC programs in access control and SoD monitoring in SAP environments — readers should not see this as a complete and unquestionable endorsement of CSI tools.

Overall, clients have shown a high degree of satisfaction with their use and implementation of CSI tools. Clients have a lot of positive feedback of the solution and find it to be a critical and sustainable platform to their future SAP access control and SoD monitoring strategies. GRC 20/20 routinely finds that clients are satisfied with CSI tools and find the organization has great customer service and rapidly addresses questions and issues. One organization reported they were very suspicious of CSI tools as they took a different approach to SAP access controls with a focus on authorization objects instead of transaction codes, but was very surprised and pleased with the results, which were always accurate.

Clients of CSI tools do see opportunity for further development and growth within the solution. Clients consistently report they would like to see CSI tools expand to support other ERP systems beyond SAP as they work in a heterogeneous environment. CSI tools has been working hard on user experience and ease of use, but some aspects of the solution organizations find take a level of technical expertise to understand that the average business user needs education on.

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