October 2014

A GLOBAL SECURITY & ASSET PROTECTION ORGANIZATION'S APPROACH TO ACCESS MANAGEMENT

How They Achieved Efficient SoD & Access Management

CASE STUDY

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.

A GLOBAL SECURITY & ASSET PROTECTION ORGANIZATION'S APPROACH TO ACCESS MANAGEMENT

How They Achieved Efficient SoD & Access Management

Executive Summary

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 ERP systems are secure and access control risks are managed in the context of a dynamic business environment. Segregation of duties (SoD), inherited rights, critical and super user access, and changes to roles are too much for today's organization to manage adequately in manual processes. A global security and asset protection organization used to manually manage their access control testing in their SAP environments. To address this challenge, they found a solution in ERP Maestro that was not only cost effective, but also enabled them to achieve their goals of efficiency, effectiveness, and agility. GRC 20/20 has evaluated and verified the use of ERP Maestro at this organization and confirms that the ERP Maestro subscription service has achieved measurable value across the elements of GRC efficiency, effectiveness, and agility. In this context, GRC 20/20 has recognized ERP Maestro with a 2014 GRC Value Award in the domain of Identity & Access Management.

Growing Need for Automated Access Controls & Segregation of Duties

Business is all about change. Change is the single greatest governance, risk management, and compliance (GRC) challenge today. Today's organization is in a continuous state of change as 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 ERP systems are secure and access control risks are managed in the context of a dynamic business environment.

Segregation of duties (SoD), inherited rights, critical and super user access, and changes to roles are too much for today's organization to manage adequately in manual processes. Surprisingly, many organizations still use these document centric and manual processes to manage access control and SoD risk. This is primarily done through spreadsheets, word processing documents, and email. 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 the business.

The challenge of managing access control in the ERP environment is burdensome when done with manual and document centric approaches. 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.

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. 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. However, automated access control/SoD solutions are known to be exorbitantly expensive and take a considerable amount of consulting resources and time to implement.

The bottom line: 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.

How a Security Organization Achieved Value in Access Management

The Situation

A global security and asset protection organization[1] used to manually manage their access control testing in their SAP environments. Prior to using ERP Maestro, they utilized a team of compliance personnel to manually validate SoD and user access (UA) concerns. This consisted of manually running multiple user reports from the SAP system and analyzing them individually. In addition, this organization implemented manual self-assessments that the business was required to complete based on each individuals roles and responsibilities within the organization.

This approach was intensively manual, prone to human error, slow, did not cover the full scope of potential risk, and rarely relied on by external audit. Most importantly, it was not continuous. External audit would perform testing of their own in the end, costing the organization additional fees and time.

This manual approach was costing this organization approximately $120,000 and 640 hours of internal resource time per SAP instance and audit cycle. Adding to this, they needed to heavily interrupt their business users to get review and feedback on access rights in the SAP environment.

1 *The focus of this case study required anonymity according to their internal policies. GRC 20/20 interviewed and researched the details presented in this research report and validated the final deliverable with the organization referenced as the case study for accuracy.*

The inefficiency cost to this global security and asset protection organization can be associated with the opportunity cost of the internal resources required to perform the access control audits on a bi-annual basis (SoD UA Validations). This was consuming their time when they could be doing other things. In addition, there was the cost of management's time to coordinate and review the process as well as the incremental cost of external auditors to validate and retest the systems. Passing access security audits became an annual gamble for the organization because of this approach, resulting in significant manual testing by external auditors due to their inability to rely on this organizations selective manual evaluations and testing.

Time and effort cost per SAP instance using OLD Manual Approach[2]

	FTE	Hours	Total Hours	Internal Cost	Total
SoD Compliance	2	180	360	$140.00	$50,400.00
Sensitive Access	1	160	160	$140.00	$22,400.00
External Audit retesting	1	120	120	$250.00	$30,000.00
Management Overhead (20%)	1	92	92	$200.00	$18,400.00
			732		**$ 121,200.00**

The Solution

This global security and asset protection organization knew something had to be done to make access control in the SAP environment not only sustainable, but also efficient, effective, and agile. To address this challenge they reviewed a range of solutions. One of their top requirements was the ability to provide a fast implementation to meet audit deadlines. However, the solutions considered were all above $400,000 in cost ($200,000 licensing with an additional $200,000 implementation and configuration cost on average). Further, the average proposed implementation time was about four to six months.

This organization found a solution that was not only cost effective, but also enabled them to achieve their goals of efficiency, effectiveness, and agility. This was in the ERP Maestro online subscription-based service. They began using ERP Maestro at on of their divisions, looking for a repeatable solution they can perform in all their other companies around the world. Most importantly, they looked to implement a solution that could help them quickly address their risk prior to an upcoming security audit. The ERP Maestro service was implemented in a couple of hours as a monthly subscription. Alternate solutions offered similar savings over doing it manually, but due to their high cost, required operating for a couple of years to see any ROI. ERP Maestro's low-cost subscription model, in contrast, was a significant and immediate savings of at least $352,800 in year one.[3] The ERP Maestro solution was able to meet their timelines and achieve access control automation. The organization was pleased, as they were then able to use the remaining budget to start addressing the remediation of identified access issues.

2 *The organization only considered the internal compliance department's cost in this calculation.*

3 *This is assuming a year one cost of up to $400,000 for an on-premise solution vs. $47,200 for ERP Maestro.*

This organization found that the subscription-based SaaS model provided a partnership mentality around implementation and ongoing support. Their feedback on ERP Maestro highlights excellent customer support provided by knowledgeable people in the SAP access space. ERP Maestro has been very responsive in addressing their queries and requests.

The Value of ERP Maestro at this Global Security Organization

GRC is a capability to reliably achieve objectives [GOVERNANCE] while addressing uncertainty [RISK MANAGEMENT] and acting with integrity [COMPLIANCE].[4] Successful GRC strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. GRC solutions should achieve stronger processes that utilize accurate and reliable information. This enables a better performing, less costly, and more flexible business environment.

GRC 20/20 measures the value of GRC initiatives around the elements of efficiency, effectiveness and agility. Organizations looking to achieve GRC value will find that the results are:

- **GRC Efficiency.** GRC provides efficiency and savings in human and financial capital resources by reduction in operational costs through 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.

- **GRC Effectiveness.** GRC achieves effectiveness in risk, control, compliance, IT, audit, and other GRC processes. This is delivered through greater assurance of the design and operational effectiveness of GRC processes to mitigate risk, 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.

- **GRC Agility.** GRC delivers business agility when 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. external risks, industry developments, market and economic factors, and changing laws and regulations). GRC agility is also achieved when organizations can identify and react quickly to issues, failures, non-compliance, and adverse events in a timely manner so that action can be taken to contain these and keep them from growing.

4 *This is the official definition of GRC found in the GRC Capability Model and other work by OCEG at www.OCEG.org.*

GRC 20/20 has evaluated and verified the implementation of ERP Maestro at this global security and asset protection organization and confirms that this implementation has achieved measurable value across the elements of GRC efficiency, effectiveness, and agility. In this context, GRC 20/20 has recognized ERP Maestro with a 2014 GRC Value Award in the domain of Identity & Access Management.

Identity & Access Efficiency Value

Using ERP Maestro, this organization has been able to identify both quantitative (hard objective facts and figures) and qualitative (soft subjective opinions and experience) measure of value as they pertain to the human and financial efficiencies they have benefited from.

GRC 20/20 has evaluated and verified the following quantitative measures of identity and access management efficiency value:

- Through ERP Maestro's SaaS deployment model there was no additional cost in hardware as well as time installing hardware in this organization's datacenter, as well as no cost in the ongoing maintenance and upkeep. The first year savings is believed to be in the area of $50,000 for hardware and maintenance alone.

- The ERP Maestro subscription, for each legal entity came at an annual cost of $47,200. That was an immediate and direct savings of 61% on top of what they were already spending by doing it manually.

- Their manual processes were costing approximately $121,200 per year. They recognized immediate as well as ongoing annual savings of $74,000 after replacing their manual effort with ERP Maestro Access Analyzer.

- In comparison to alternate solutions they considered, the lower cost of ownership of ERP Maestro saved them $200,000 per SAP instance in just software licensing. The organization further estimates that it saved another $200,000 on consulting services for the implementation and setup of other solutions. This totals what the organizaiton believes to be a $400,000 cost just to implement alternative solutions versus total annual costs of $47,200 for the ERP Maestro online subscription service.

- Savings in external audit who used to do all the access control testing themselves is $50,000 a year.

- The organization sees further value moving forward as the SaaS model means they are continuously upgraded to the latest release and do not have to undertake the cost of an upgrade project every three to five years.

- In 1 hour, ERP Maestro completes what used to take 732 hours before when they performed it manually.

- Overall, the organization estimates that they have a net annual recurring savings of $74,000 per SAP instance (after paying ERP Maestro subscription fees) over their previous manual approach because they no longer need to dedicate internal resources to perform the same activity.

- While it is difficult to measure and put a value to, the organization states they have a cost savings of avoiding a significant security event such as fraudulent activity related to segregation of duties.

- With a subscription model, they do not need to pay for an FTE resource to maintain an access control solution.

- The organization can now assign freed up resources to more productive tasks. They freed up two staff resources and one management level resource that are now able to focus on other priorities.

GRC 20/20 has evaluated and verified the following qualitative measures of identity and access management efficiency value:

- The access control testing is now completely automated.

- The ERP Maestro solution saves the time for business stakeholders through intuitive reporting with the right information that empowers business owners to own the risk.

- The ability ERP Maestro gives the organizaiton to perform iterative testing, drastically improves efficiency of the process.

Identity & Access Effectiveness Value

Using ERP Maestro, this organization has been able to identify both quantitative (hard objective facts and figures) and qualitative (soft subjective opinions and experience) measures of value as they pertain to the effectiveness of access management that they have benefited from.

GRC 20/20 has evaluated and verified the following quantitative measures of identity and access management effectiveness value:

- With the quick implementation and results of testing, this organization was able to start their access control remediation project four to six months early that enabled them to meet some critical audit deadlines. Their remediation team could begin addressing the conflicts immediately which was possible with their manual approach or with any other vendor they evaluated.

- ERP Maestro has enabled 100% testing coverage of all users, roles, SoD rules and sensitive access rules, where before it was a small sample set.

- The Role Remediation abilities built into each report, improve the organization's remediation decision making tenfold.

GRC 20/20 has evaluated and verified the following qualitative measures of effectiveness value:

- ERP Maestro's ability to perform impact assessment on users who have actually executed a risk is highlighted by the solution which allows them to focus on a small subset of the highest risk areas.

- External auditors and management have greater confidence and reliance on the results of access control testing.

- The ERP Maestro solution was able to deliver results with a very low rate of false positives.

- The organization has achieved continuous Sarbanes-Oxley control testing to access and security requirements with a noticeable reduction in control deficiencies.

- The organization states they have increased SoD visibility by the business.

- External auditors place higher reliance on the ERP Maestro testing over their manual approach, this has actually created a relationship in which there is greater collaboration and comfort between their internal control teams and external audit.

- Simplicity and reliability of generating access control testing results has created strong buy-in from business stakeholders.

- Total visibility into the extent of issues discovered by ERP Maestro enables a quick ability to react to security issues, such as drill down abilities in to the authorizations themselves that cause the issue. This means reduction in wasted time chasing issues in investigations.

Identity & Access Agility Value

By using ERP Maestro, this organization has been able to identify both quantitative (hard objective facts and figures) and qualitative (soft subjective opinions and experience) measures of value as they pertain to the agility and responsiveness of access management they have benefited from.

GRC 20/20 has evaluated and verified the following quantitative measures of identity and access management agility and responsiveness value:

- The organization has moved from periodic assessments of small sample sets of user access to 100% review of all user access though continuous monitoring of their SAP environment in twenty-four by seven three-hundred sixty-five days a year situational awareness.
- The organization's previous approach was not agile because it was cumbersome, it involved a manual process costing 732 hours of time and $121,200 and was not a repeatable process they could introduce across their business divisions. ERP Maestro allowed them to easily and simply plug the solution into other SAP instances.
- This organization is constantly changing – connecting ERP Maestro to other instances requires a 5 minute configuration change. Alternative solutions required an implementation project that took a significant amount of time counted in weeks to months which was not sustainable.

GRC 20/20 has evaluated and verified the following qualitative measures of agility and responsiveness value:

- This organization reports an ability to make quick decisions in the context of access reviews and in a dynamic and demanding business environment.
- ERP Maestro's ability to present the right information in the right way has improved adoption of ERP Maestro across their SAP environment.
- ERP Maestro's risk prevention capabilities allow risks to never enter their environment, which means no need to later remediate.
- The organization has seen an ongoing and sustainable reduction of access risk in an environment that grows more complex and changes constantly.
- A specific agility value proposition was the ability to have business take ownership of access risks and decisions through ERP Maestro's intuitive reporting and presentation of findings.
- The ERP Maestro support team has proved to be agile to adjust the solution as the business changes.
- The organization reports they now have a streamlined process that is simple to communicate change requirements to the IT department

GRC 20/20's Final Perspective

This global security and asset protection organization is amazed that access control reviews can be so . . . simple. They have found the ERP Maestro solution to be exceptionally robust while being a SaaS solution in the cloud with no complicated software to install and setup. ERP Maestro was able to be setup in just a couple of minutes to connect the solution into their SAP environment enabling a full automated access control suite when they had none before. The organization claims that ERP Maestro's greatest strength is their ability to provide such a premium service, so quickly and for such a low cost.

Due to the architecture and flexibility (agility) of the ERP Maestro solution, the organization will be able to leverage the solution across all of their SAP ERP environments. It was not possible to do this before due to their constantly shifting organizational structure and the constant implementation work that would be required to "keep up" that competitive solutions required. It was also practically impossible due to the cost of such an exercise. They are now positioned to consider a full deployment across all of their operating companies running SAP. This will enable their risk organization to focus their GRC efforts around a core software set, and enable them to effectively and efficiently address any concerns that may arise. Most importantly – the organization now has a means to continually audit their Access Control environment and achieve sustainable compliance.

About GRC 20/20

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