Carlisle Construction Materials

Value Achieved in Automated Controls in an SAP Environment

VALUE 2016

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.

Carlisle Construction Materials
Value Achieved in Automated Controls in an SAP Environment

Growing Need for Automated Access Control & 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.

Carlisle Construction Materials:
Value Achieved in Automated Controls in an SAP Environment

The Challenge Carlisle Construction Materials Faced

Carlisle Construction Materials (CCM) is a case in point. CCM is a diversified manufacturer and supplier of premium building products for the commercial and residential construction markets. CCM offers sustainable, eco-friendly products that help reduce a building's carbon footprint, and often minimize its energy consumption and costs. CCM, a division of Carlisle Companies (NYSE:CSL), has annual revenues of $2 billion, employs over 2,400 people, and operates 24 plants in North America and five in Europe.

Due to consistently poor audit findings, CCM knew their SAP environment was not audit ready or in a healthy state of compliance. CCM's internal IT team attempted to remediate their security issues by themselves through manual processes. This process took months to compile with an end result in poor data, while failing to remediate their security issues. CCM had employed a part-time internal SAP security resource that made security changes which resulted in a very complex security model with over 3,000 roles for CCM's 700 users.

CCM had deployed a SoD solution, but the output was indecipherable and the tool failed to provide a clear path for remediation. The solution's inadequate customer support left CCM unsure of how to proceed with the output. With each annual audit, the number of SoD risks consistently increased and CCM would try to manually remediate those risks. Unfortunately, upon retesting, auditors would find that more SoD risks were added than remediated. To better understand how to architect the best approach and "get clean," CCM knew they needed automated GRC tools and expert support.

Due to lengthy, manual processes, CCM was wasting hundreds of hours every year preparing for and responding to external audits. To prepare for each audit, CCM would pull user access data and supporting documentation for various IT audit validation tasks: a data gathering task that took two or more months. This raw data would then be translated into Excel Workbooks, printed, and stored in folders. The printed copies were often 20 or more pages per role. CCM describes this process as "a nightmare," as they had to perform this process for over 3000 roles. This entire process would be repeated if even a minor adjustment was needed to the workbooks. External auditors would then be onsite for two to four weeks, reviewing user access data often laced with inaccuracies or errors. Because the auditors were not able to rely on CCM's existing SoD tool, they would

use their own tools to analyze the data and find numerous issues. This additional SoD review process alone would result in significant audit fees which were $4,000 on average for each occurrence. This process was repeated after fruitless remediation attempts. To CCM, it felt like a never ending cycle. Trying to mitigate risks company-wide became an impossible task. Managers were expected to print and maintain all supporting documentation for audit purposes and address any issues. Due to the manual nature of this approach, it was often forgotten or completed incorrectly and wasted hundreds of hours producing unreliable results. CCM knew there had to be a better approach.

Solution to Carlisle Construction Material's Problem

To address this problem, CCM evaluated and purchased the ControlPanelGRC® Access Controls Suite in late 2013 and completed their remediation efforts in 2014. ControlPanelGRC is a Governance, Risk, and Compliance (GRC) solution provider of automated and continuous control monitoring and enforcement for SAP environments. ControlPanelGRC automates time-consuming tasks associated with compliance reporting and audit support through rapid implementation, integration with SAP, reporting and analytics, and an intuitive user experience.

ControlPanelGRC's Access Controls Suite provides intelligent management of SAP user access. The Access Control Suite enables organizations to quickly assess potential compliance failures, remediate SoD conflicts, and control access to SAP environments by preventing excessive user access. Through workflow and automated utilities, ControlPanelGRC supports continuous compliance reporting. With the use of the Accelerated Remediation Toolkit that is part of ControlPanelGRC's Access Controls Suite, organizations are able to successfully complete security remediation or redesign projects in a condensed timeline and under budget.

To assist CCM, the ControlPanelGRC Team architected the Accelerated Remediation Toolkit and related methodology prior to the start of the remediation efforts to help reduce the timeline of the overall project, allowing CCM to show significant progress to external auditors before 2015 IT audit tasks were started. The solution has been a success for CCM, which has also now implemented other components of ControlPanelGRC to help automate other parts of GRC.

The short-term benefits to CCM they achieved in the first-year of implementation were:

- ■ **Reduction in external auditor time.** External auditors can now access the ControlPanelGRC system and run reports themselves. Reports that used to take four hours or longer to generate, now run in less than a minute. The auditors are impressed with the speed of the ControlPanelGRC solution at CCM.

- ■ **Reduction in SoD risks.** All SoD risks at CCM have been identified and remediated or mitigated with automated compensating controls.

- ■ **Streamlined mitigation processes.** The Accelerated Remediation Toolkit enabled CCM to transform its company-wide manual processes to a single control

monitor within the finance group, who is able to pull supporting documentation themselves.

- ■ **Rapid remediation.** ControlPanelGRC significantly condensed the security remediation projects by providing automated tools and a clear path to get clean with limited impact on the end-users.

- ■ **Simplified SAP security model.** CCM's final security design included 70 primary roles, with location specific versions, that are understandable by non-technical users: a decrease from 3000 roles.

- ■ **Reduced costs.** Using the Accelerated Remediation Toolkit, CCM was able to reduce SAP security consulting costs by 80%, SAP security administration costs by 75% per year, and external IT audit costs by an estimated 50% per year.

The projected ongoing long-term benefits for CCM over three to five years are:

- ■ **Audit confidence.** CCM is able to be proactive in the audit process, rather than reactive. CCM's internal team is able to identify and remediate issues before they are discovered by the external auditors. Now, the IT department is considered a thought leader by dramatically reducing the number of adverse audit findings.

- ■ **Reduced audit preparation.** The company-wide manual data and documentation gathering processes required for audit preparation has been eliminated, saving hundreds of hours for CCM.

- ■ **Continued cost savings.** CCM is realizing a reduction of SAP security administration costs by 75% per year and external IT audit costs by an estimated 50% per year.

- ■ **Increased risk mitigation.** Over the next three to five years, CCM is hoping to mitigate even more risks with increased automated controls.

- ■ **Staying clean.** CCM now has the ability to maintain a compliant SAP environment and will not require another security remediation project.

Value Achieved in GRC Efficiency, Effectiveness, and Agility

GRC is an integrated capability to reliably achieve objectives [GOVERNANCE] while addressing uncertainty [RISK MANAGEMENT] and acting with integrity [COMPLIANCE].[1] 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.

---

1   *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 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.

GRC 20/20 has evaluated and verified the implementation of ControlPanelGRC at CCM 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 ControlPanelGRC and CCM with a 2016 GRC Value Award in the domain of Automated and Continuous Controls.

GRC Efficiency Value

Using ControlPanelGRC, CCM 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. These include:

- Reduced SAP security consulting costs for the remediation projects by 80%.

- Reduced manual testing processes of SAP security roles by 85%.

- Reduced SAP security administration costs by 75% per year.

- Reduced external IT audit costs by an estimated 50% per year.

- Eliminated unmitigated SoD risks.

- Reduced overall security remediation timeline to four months.

- Reduced over 3000 roles to 70 primary roles and 350 location specific roles.

- CCM experienced time to value by condensing the implementation time to one week, and overall remediation project to less than 4 months.

- Reduced manual processes by eliminating hours of monthly reporting and audit preparation for multiple teams across the organization.

GRC Effectiveness Value

Using ControlPanelGRC, CCM has been able to identify both quantitative and qualitative measures of value as they pertain to the effectiveness of access management that CCM has benefited from.

- Eliminated unmitigated SoD risks.

- CCM now has the ability to model user access changes, which reduces the chance of new SoD risks being added to their environment.

- CCM no longer has to rely on their auditors to identify SoD risks in their environment.

- CCM has audit confidence in that they are prepared and know they will successfully pass audits.

- CCM is no longer living in fear of audits because they can immediately analyze all risks and verify that all compensating controls are being reviewed in a timely manner.

- CCM's IT organization has become a thought leader in the business as related to setting up a powerful internal control structure.

- CCM now has a true automated controls framework in place.

- CCM now has a self-documenting, automated IT internal control structure that has saved hours of manual processes.

- CCM now has peace of mind—the company is confident that ControlPanelGRC is proactively identifying potential access control risks.

- The IT department is considered a thought leader by dramatically reducing the number of adverse audit findings.

- CCM's internal team is able to identify and remediate issues before they are discovered by the external auditors.

GRC Agility Value

By using ControlPanelGRC, CCM 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.

- CCM can now immediately identify access control risks and has a better understanding of how those risks can impact the overall health and continuous success of the company if they are not properly mitigated.

- CCM now has audit confidence and is proactive in the audit process, rather than reactive.

- Automated identification of remediation options by allowing the Accelerated Remediation Toolkit to identify the appropriate path to "get clean".

- At the end of one week of training and implementation, the ControlPanelGRC Accelerated Remediation Toolkit was live and ready to start the security remediation project.

- Reduced end-user frustration with the security remediation efforts by providing a simple restore to their original security for instances where a user was not able to execute critical job responsibilities using their new security.

- Reduced time to resolution for end-user security issues with most defects being resolved on the day they were identified.

- CCM's internal and external auditors are now able to rely on the real-time reporting within ControlPanelGRC.

GRC 20/20's Final Perspective . . .

ControlPanelGRC's Accelerated Remediation Toolkit has provided CCM with significant cost reductions for their internal auditors, external auditors, SAP security consultants, and SAP security administrators. CCM was able to achieve these cost reductions in a very short timeframe, while providing an internal control structure that provides them with confidence going into their audits. Through this remediation project, CCM has significantly reduced IT access risks, automated related compensating controls, and from an IT audit perspective, become a thought leader within its larger organization.

CCM is in a better position for completing successful audits, staying risk free and compliant in order to support the organization's overall company goals (which include international business growth) with an enhanced internal controls structure. The Accelerated Remediation Toolkit helped them "get clean" and setup a continuous controls monitoring infrastructure for them to "stay clean".

CCM has better visibility into potential risks in their environment and confidence in their controls infrastructure. Their strong sense of audit confidence allows them to be proactive, finding issues before audits, rather than being reactive to issues identified by external auditors. Having the confidence that their SAP environment will "stay clean" assures them that another security remediation project will not be required. As part of the project, CCM was able to greatly simplify their security infrastructure, which not only makes it easier on access requestors and approvers, but reduces the security administration requirements. Lastly, CCM was able to automate compensating control reporting and monitoring, which eliminated time consuming, often erroneous, manual processes.

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.