soterion

SAINT-GOBAIN

case study

SAP SECURITY: DEALING WITH CROSS-DIVISION ACCESS IN SAINT-GOBAIN

Access control at a company in a class of its own

Access control in SAP is a challenge in any context. Having multiple companies within a shared SAP ecosystem created a unique set of access control issues for Saint-Gobain South Africa.

In this article, we'll share the highlights of Saint-Gobain SA's journey to SAP authorization compliance, specifically how they managed cross-division access control.

SAP Access Control in a Group of Companies

Access control in a group of companies that use SAP presents a specific set of problems, namely:

- *Consistency in role methodologies:* Large groups like Saint-Gobain often suffer from inconsistencies in the way that SAP role design is determined and implemented. It is often a case of "too many cooks spoil the broth" and the use of outsourced resources.
- *Cross-division access control:* Users often retain access rights they should no longer have as they move between companies and roles. Risks can't be effectively addressed if there is no regular user review to mitigate authorization creep.

Saint-Gobain – a tradition of high standards

The Saint-Gobain Group was founded in 1665 as one of 25 royal mirror-glass manufacturing companies and has a rich history of over 350 years. Saint-Gobain expanded its operations into other materials and brands as the demand for glass and other building materials grew during after the industrial revolution.

Today, Saint-Gobain is present in 67 countries with more than 180 000 employees. The company designs, manufactures and distributes materials and solutions which are key ingredients in the wellbeing of each of us and the future of all. They can be found everywhere in our living places and our daily life: in buildings, transportation, infrastructure and in many industrial applications. They provide comfort, performance and safety while addressing the challenges of sustainable construction, resource efficiency and climate change.

The case of the leaky Chinese wall

Four divisions and surprise audits

Saint-Gobain SA consists of several business divisions. Four of the divisions (Weber, Gyproc, ISOVER and PAM) access a single SAP ECC system with a requirement to restrict cross-business activity access. An employee of one business activity should not have access to any of the other business activities with this restriction in place.

As part of their efforts to maintain their high standards, Saint-Gobain has a powerful group-wide internal audit department. They are mandated to perform surprise audits on a regular basis with typically only one-month notice. Most of the attention in such audits is focused on user access (specifically wide and cross-business activity access) due to the nature of the group.

The company being audited receives a grade at the end of the audit based on one of the following process grades:

Grade	Description
A	Control in place, efficient and formalized. The risks are properly mitigated.
B	Control in place but not fully efficient and/or issues noted in terms of formalization. There is limited residual risk exposure.
C	Control in place but incomplete. There is some remaining risk exposure.
D	Inefficient control. There is significant remaining risk exposure.
E	No control. There is ongoing high-risk exposure

The challenges of outsourcing and authorization creep

Saint-Gobain SA initially adopted SAP in 2001 and faced several challenges, consistently failing their access control audits.

The first challenge was the access control methodology that was selected during the initial SAP implementation. The job-based roles were too broad and provided too much access to users.

Typical of most companies running SAP, Saint-Gobain SA also had a challenge with “authorization creep” where users inherited additional access as they moved internally between jobs and business units within the group. As the user moved to a new position there would be a handover period where they would require temporary access to their previous role. However, since there was no access risk solution to highlight these risks, access would often remain in place. This resulted in a “leaky Chinese wall” between the companies

Saint-Gobain SA made use of an SAP authorization outsourced provider to perform technical functions such as role changes. Using an outsourced provider yielded two unexpected challenges:

- The service provider operated on a basis of executing their approach only, and never offered any indication of best practices. As role changes were applied, many of the risky practices became ingrained in the system.
- The outsourced provider changed security resources a number of times. This caused inconsistencies in role methodologies as each resource had a preferred approach.

Without an access risk solution, there was no visibility of the access risk impact of the SAP access change request.

SAINT-GOBAIN

Taking on the GRC Journey

Strong foundations similar to a multi-story building

After evaluating a number of possible SAP access risk (GRC) solutions, Saint-Gobain SA selected and implemented the Soterion solution in 2015. However, implementing an access risk solution was not the silver bullet that Saint-Gobain SA was expecting.

> Saint-Gobain SA were still failing audits due to users having cross-division access even though an access risk solution was in place.

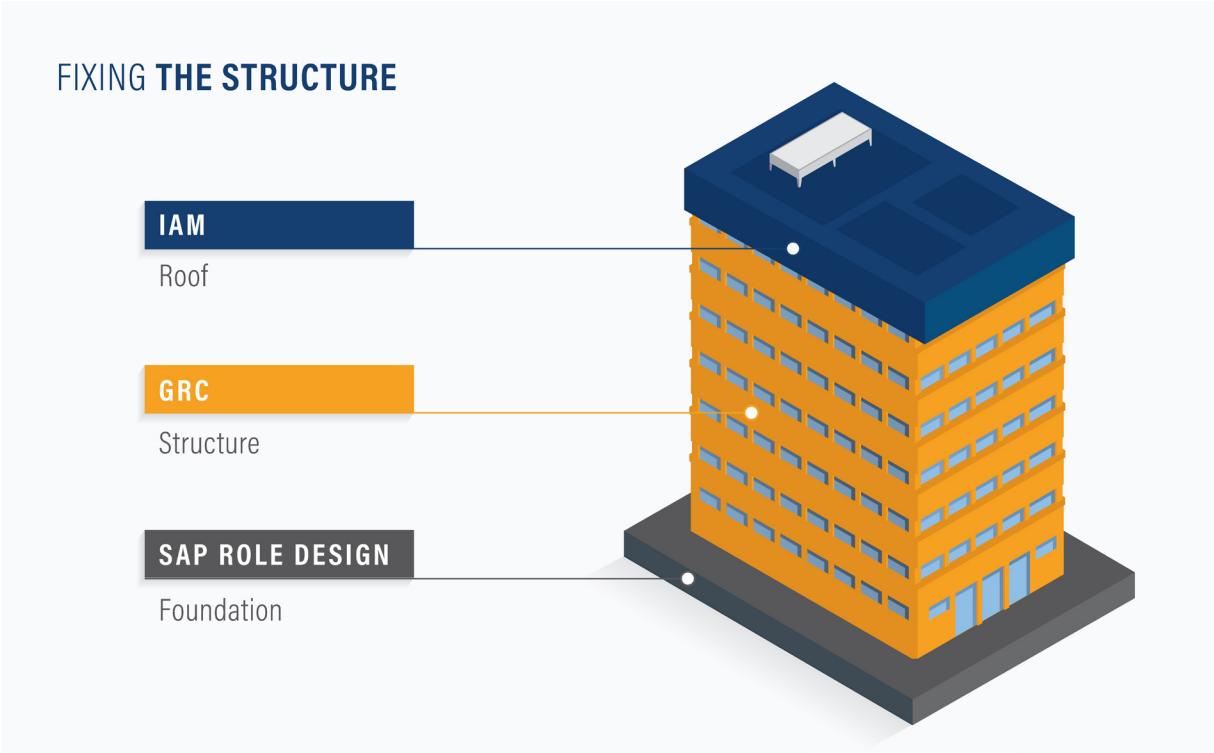
Saint-Gobain SA was passionate about implementing good SAP security. They realized that they needed more than just a technical access risk solution and approached Soterion for assistance in understanding and fixing the underlying problems.

Two critical issues were highlighted during the initial consultation with Soterion:

- Saint-Gobain SA had a mix of role methodologies which made the assignment of appropriate role access overly complicated.
- The risk assessment indicated many roles that had cross-division access, creating a "leaky Chinese wall" between the different divisions.

Robust access control can be compared to a multi-story building. A strong foundation requires good role design for both business and technical roles.
The organization benefit from a GRC solution as soon as a strong foundation is in place.

Once a solid role design and GRC principles are in place, the next level of Identity Access Management (IAM) can be implemented, promoting and ensuring fine-grained control of access.



A GRC turnaround roadmap

Role redesign

In SAP there are various approaches to role design, each with their own unique set of pros and cons. A comparison was done for Saint-Gobain SA between a derived role methodology and a task/value role methodology. The following outcome was determined based on Saint-Gobain SA's requirements:

Role Design Methodology	Pros	Cons
Derived	• Well-known methodology	• If small (functional) roles are created, you end up with many roles derived for each Organizational Level or controlling field • Support intensive
Task and Value	• Fewer roles, better visibility of user access • Easier risk remediation for superfluous roles • Fine-grained or appropriate assignment of access	• Not a well-known methodology • Requires more advanced security administrators to keep solution robust
Composite	• Easy maintenance or support	• Minimal flexibility, wider access (more risk)

> A primary requirement for Saint-Gobain SA was to find a balance between flexibility and control in their role design. Saint-Gobain SA decided on creating smaller functional or task roles (e.g. Purchase Order Processing) to provide the necessary level of flexibility.

The derived role methodology was rejected due to the vast number of roles that Saint-Gobain would have ended up with, based on the number of controlling field values (Company Codes or Plants, etc). Ultimately the role methodology chosen was based on "task and value" which would be applied to business and technical roles.

In line with the role types, the project was split as follows:

- *Business End User roles:* Using the User-Transaction logs (SM20), task roles were assigned to the users based on historical data in combination with line manager approval. A number of functional roles were identified and applied as business roles. This allows for ease of change if required. Organizational level access was provided via value roles.
- *Technical roles (Phase 1):* Appropriate task roles related to technical job functions (e.g. Basis, authorization administration, etc.) limited the risk of wide access given to internal support personnel and outsourced providers.
- *Technical roles (Phase 2):* Restriction of basis critical authorization objects, with a special focus on implementing fine-grained Remote Function Call (RFC) access.

Rule-set customization

Rule-sets are combined rules that are attached to identified GRC risks. They are implemented as a means to link mitigating controls to the risks associated with business processes. Soterion developed a standard rule-set that needed to be adapted to suit Saint-Gobain SA's needs. The Soterion solution was implemented with a market-leading access risk rule-set. However, as with all standard or out-of-the-box rule-sets, they are designed to be applicable to organizations across different industries and geographies. Customizing the rule-set to be Saint-Gobain SA specific was an important step in the journey to ensure business buy-in.

Mitigations

As it is impossible to operate without any access risk, mitigations play a vital role in reducing the organization's risk exposure. It was important to mitigate those risks that were unavoidable and relevant to the organization. Many controls already existed in the business. These controls were identified and documented into a central repository, and mapped to risks in the customized rule-set.

Business Education

Part of the solution was educating line managers on risks and mitigating controls relevant to their area of responsibility, promoting ownership. Business unit heads were trained to understand what they were reviewing so that they can make informed business decisions, thus promoting a culture of risk awareness in the organization.

Emergency Access Management

In certain circumstances, business and support users require temporary or ad-hoc (emergency) access to perform business-critical activities.
Saint-Gobain SA implemented Soterion's Elevated Rights Manager to manage sensitive and emergency access. This module ensures both support and business users have access to sensitive functions when required in a controlled manner. Elevated Rights sessions are logged and their activity sent to owners for review

Continuing the journey: Next steps for Saint-Gobain SA

Proper GRC management is an ongoing process. Every GRC journey has as its goal flexible, effectively controlled user access rights management.

The next steps in the journey for Saint-Gobain SA are:

- User access reviews: Implementing an access request, review and approval process.
- Identity management: As an additional layer to provide fine-grained access control, Saint-Gobain SA will consider the business case for an identity access management solution.

GRC as a Managed Service

More than outsourcing

An SAP system is constantly changing as the organization evolves. Employees move between departments, new employees join, and in the case of a group of companies, employees sometimes move to sister companies. User access needs to change with every movement of an employee, but without appropriate support, they often remain incorrectly assigned. Saint-Gobain SA understand the reason for their SAP authorization challenges prior to their GRC journey and want to ensure that the solution stays in good shape. They understand that much of the integrity of their authorization solution relies on the abilities of their outsourced provider to implement best practices in line with the new approach.
The failures experienced with previously outsourced providers highlighted that they are not just wanting to outsource authorizations. Instead, they are looking for a more comprehensive offering: GRC as a managed service.

What is GRC as a managed service?

GRC as a managed service is a relationship between the service provider and client that contributes expertise along with technology to fulfil certain needs. It isn't just outsourcing technical activities - it is a partnership where the service provider looks after the client as if they are part of the organization. For SAP GRC, a managed service extends beyond standard SAP authorizations to include risk, controls and audit support. As Saint-Gobain SA matures on their GRC journey, their internal expertise has allowed them to bring some of the activities in-house. This means that they no longer need to rely fully on the outsourced support to perform authorizations functions. Instead, only role content changes now need to be outsourced, while the allocation of roles is handled internally. As part of this development, Saint-Gobain SA introduced an internal controls department. This has allowed ownership to move away from IT to the business, giving process owners better insight into, and control over, the risks within their domains.

> For Saint-Gobain SA there was a constant challenge around access control to their SAP systems. They didn't have a clear view of their access risk and suffered from authorization creep. The problems they experienced were further compounded by outsourced partners who performed technical functions on request, rather than guiding them towards best practices. In fact, with the change of every outsourced resource, different role design methodologies made it overly complicated to manage role access. All these issues were reflected in the results of surprise audits, which they often failed.
> After engaging with Soterion, Saint-Gobain SA was prepared for audit success through the role redesign. With a better understanding of business risks, along with a higher degree of access control, process owners developed more business accountability. The Soterion solution provides business unit heads with more visibility, control and management buy-in. Governance, Risk and Compliance is a continuous journey. With the support of Soterion, Saint-Gobain SA has established a sound basis for their authorizations and a clear roadmap ahead.