soterion

SAINT-GOBAIN

étude de cas

SÉCURITÉ SAP: GÉRER L'ACCÈS AUX DIFFÉRENTES DIVISIONS DE SAINT-GOBAIN

Contrôle d'accès dans une entreprise de grande renommée

Quel que soit le contexte, le contrôle d'accès dans SAP est un véritable défi. Le fait d'avoir plusieurs entités partageant le même écosystème SAP a apporté son lot de complications à Saint-Gobain Afrique du Sud en matière de contrôle d'accès.

Dans cet article, nous vous proposons de découvrir les temps forts de sa mise en conformité avec le processus d'autorisation SAP, en particulier en ce qui concerne la gestion des accès aux différentes divisions.

Contrôle d'accès SAP au sein d'un groupe de sociétés

Le contrôle d'accès au sein d'un groupe de sociétés utilisant SAP pose un certain nombre de problèmes, notamment :

- *L'homogénéité des méthodologies en matière de rôles:* Les grands groupes comme Saint-Gobain présentent souvent des incohérences dans la façon dont les rôles SAP sont conçus et mis en œuvre. C'est généralement ce qui arrive lorsqu'on fait appel à des prestataires externes et si tout le monde veut apporter son grain de sel.
- *Le contrôle des accès transverses:* En cas de mobilité interne, les utilisateurs conservent souvent des accès auxquels ils ne devraient plus avoir droit. Les risques ne peuvent pas être traités de manière efficace si les fichiers utilisateurs ne sont pas régulièrement vérifiés afin de limiter ces « glissements » d'autorisation.

Saint-Gobain : un niveau d'exigence traditionnellement élevé

Créé en 1665 comme l'une des 25 manufactures royales de glaces de miroirs, le Groupe Saint-Gobain repose sur plus de 350 ans d'histoire. Avec la révolution industrielle et la demande croissante en verre et autres matériaux de construction qui l'accompagne, Saint-Gobain développe ses activités à travers d'autres produits et d'autres marques.

Aujourd'hui, Saint-Gobain compte plus de 180 000 collaborateurs et intervient dans 67 pays. L'entreprise conçoit, fabrique et distribue des matériaux et des solutions devenus des éléments incontournables de notre bien-être et de notre avenir à tous. Présents partout, ils font partie de notre environnement quotidien : dans les immeubles, les transports, les infrastructures, et pour de nombreuses applications industrielles. Ils allient confort, performance et sécurité tout en répondant aux exigences de la construction durable, de l'efficacité des ressources et du changement climatique.

Un exemple de perméabilité
Quatre entités et des audits à l'improviste

La filiale sud-africaine de Saint-Gobain comporte plusieurs entités. Quatre d'entre elles (Weber, Gyproc, ISOVER et PAM) partagent le même système SAP ECC, avec un accès nécessairement limité à ses propres activités. Avec cette restriction, un collaborateur appartenant à une division ne devrait pas avoir accès aux activités des autres entités.

Engagé à maintenir son haut niveau d'exigences, Saint-Gobain dispose d'un puissant service d'audit interne qui opère à l'échelle du Groupe. Ses auditeurs sont mandatés pour effectuer régulièrement des contrôles à l'improviste, annoncés seulement un mois à l'avance en général. En raison de la nature du Groupe, l'accès des utilisateurs (en particulier à l'échelle du système et en ce qui concerne les accès transverses) est la préoccupation principale lors de ces audits.

Au terme de l'audit, une note est attribuée à l'entité expertisée sur la base des critères suivants :

Note	Description
A	Contrôle en place, efficace et formalisé : les risques sont réduits de manière appropriée.
B	Contrôle en place mais pas pleinement efficace et/ou problèmes décelés en matière de formalisation : le système est exposé à certains risques résiduels.
C	Contrôle mis en place incomplet : le système est encore vulnérable.
D	Contrôle inefficace : le système est encore exposé à un nombre significatif de risques.
E	Contrôle inexistant : le système est constamment et fortement exposé aux risques.

Le défi de l'externalisation et le glissement d'autorisations

Depuis l'adoption de SAP en 2001, Saint-Gobain Afrique du Sud a rencontré plusieurs difficultés dues aux échecs répétés de ses audits en matière de contrôle d'accès.

Le premier obstacle a été la méthodologie appliquée au contrôle d'accès qui avait été choisie lors de la mise en œuvre initiale de SAP. Les rôles basés sur des tâches étaient trop larges et accordaient trop de droits d'accès aux utilisateurs.

À l'instar d'un grand nombre d'entreprises qui utilisent SAP, Saint-Gobain Afrique du Sud a également été confronté à un « glissement » d'autorisations, où les utilisateurs héritaient d'un accès supplémentaire lorsqu'ils changeaient de poste ou d'unité opérationnelle au sein du Groupe. En cas de mobilité interne, une période de passation avait lieu durant laquelle l'utilisateur devait avoir accès, temporairement, à son rôle précédent. Cependant, comme aucune solution ne permettait de déceler les risques d'accès, il n'était pas rare que les accès restent en place, ce qui donnait lieu à une certaine forme de perméabilité entre les entités.

La filiale sud-africaine a fait appel à un prestataire externe spécialisé dans les autorisations SAP pour effectuer des opérations techniques, telles que la modification de rôles. Le recours à un sous-traitant a engendré deux complications imprévues :

- Le fournisseur est intervenu en suivant son approche uniquement, sans jamais proposer de bonnes pratiques. Après modification des rôles, une large part des pratiques à risque ont pris racine dans le système.
- Le prestataire externe a modifié les ressources utilisées pour la sécurité plusieurs fois, ce qui a provoqué des incohérences dans les méthodologies employées pour la création de rôles car chaque ressource impliquait une approche privilégiée.

Sans solution pour gérer les risques d'accès, l'entreprise n'avait aucune visibilité sur l'incidence d'une demande de modification d'accès SAP sur ces risques.

SAINT-GOBAIN

Le début de l'aventure GRC

Des fondations solides, comme pour un immeuble

Après évaluation de plusieurs outils consacrés aux risques d'accès SAP (GRC), Saint-Gobain Afrique du Sud a sélectionné et installé la solution Soterion en 2015. Néanmoins, la mise en œuvre d'une solution de gestion des risques d'accès n'a pas été le remède miracle que Saint-Gobain attendait pour sa filiale sud-africaine.

> Saint-Gobain Afrique du Sud ne parvenait toujours pas à réaliser des audits valables en raison d'utilisateurs dotés d'accès transverses malgré la mise en place d'une solution consacrée aux risques d'accès.

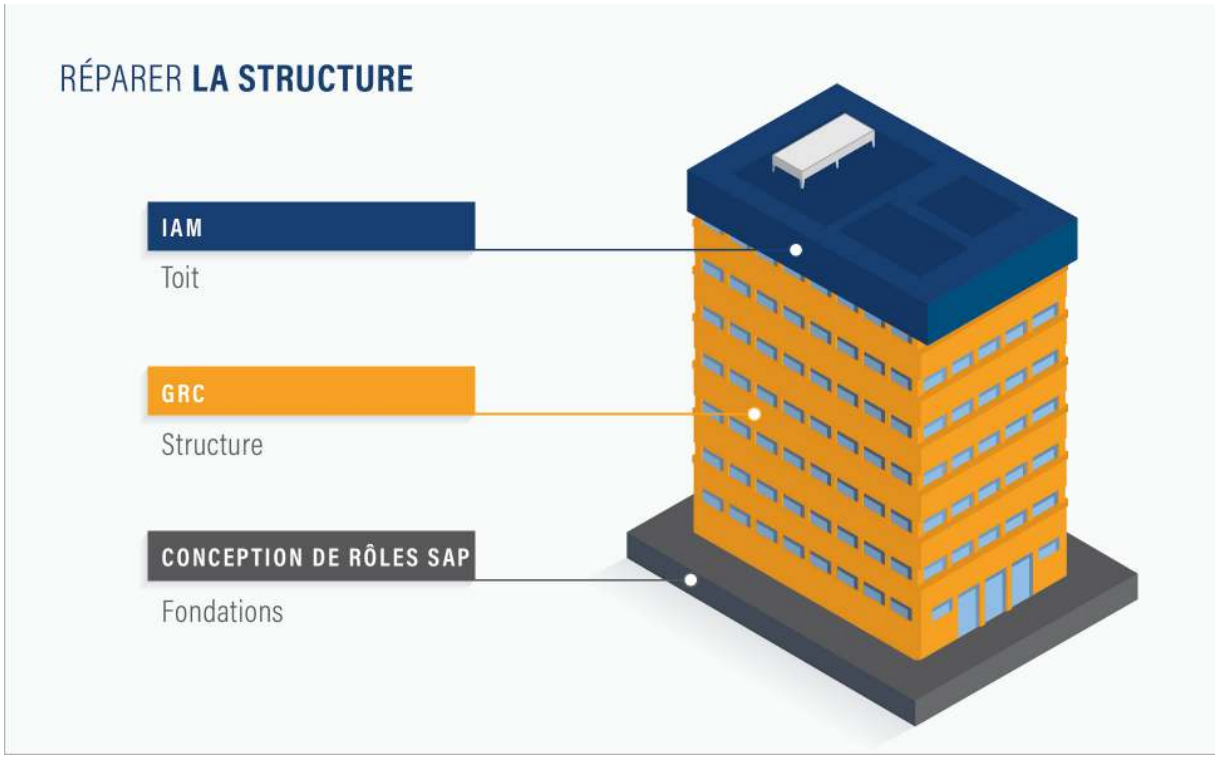
Saint-Gobain Afrique du Sud s'est montré très enthousiaste à l'idée d'instaurer une sécurité SAP efficace. Les équipes ont réalisé qu'un simple outil technique ne suffisait pas pour gérer les risques d'accès. Elles se sont donc tournées vers Soterion dans le but de comprendre et résoudre les problèmes sous-jacents.

Deux obstacles sérieux ont été mis en avant lors de la première consultation avec Soterion :

- L'application de méthodologies variées pour la définition de rôles, ce qui rendait l'attribution des accès trop compliquée ;
- Le grand nombre de rôles dotés d'accès transverses, d'après l'évaluation des risques, ce qui créait une certaine perméabilité entre les différentes divisions.

Un contrôle fiable des accès peut être comparé à un immeuble de plusieurs étages. Pour des fondations solides, il est nécessaire de bien concevoir les rôles, tant techniques qu'opérationnels. L'entreprise bénéficie d'une solution GRC dès lors que des fondations solides sont en place.

Après la mise en place d'une conception ferme des rôles et l'application des principes de GRC, la prochaine étape est la gestion d'identités et d'accès (Identity Access Management ou IAM) afin d'encourager et d'assurer un contrôle détaillé des accès.



Un plan d'action pour redresser la GRC

Une nouvelle dé inition des rôles

Dans les PAS, il existe différentes approches de la conception des rôles, chacune ayant son propre ensemble d'avantages et d'inconvénients. Une comparaison a été faite pour Saint-Gobain SA entre une méthodologie de rôle dérivé et une méthodologie de rôle de tâche/valeur. Le résultat suivant a été déterminé sur la base des exigences de Saint-Gobain SA :

Méthode de création des rôles	Points positifs	Points négatifs
Rôles dérivés	• Méthode bien connue	• S'il s'agit de petits rôles (fonctionnels) à créer, on se retrouve avec de nombreux rôles dérivés pour chaque niveau organisationnel ou domaine de contrôle. • Assistance vitale
Rôles associés à des tâches et des valeurs	• Moins de rôles, plus de visibilité des accès utilisateurs • Compensation des risques facilitée pour les rôles superflus • Attribution appropriée ou minutieuse des accès	• Méthode peu connue • Nécessite des administrateurs sécurité plus avancés pour maintenir la fiabilité de la solution
Rôles composites	• Faible niveau de maintenance ou d'assistance	• Flexibilité limitée, accès plus large (risque accru)

> L'une des principales exigences de Saint-Gobain Afrique du Sud était de trouver le juste milieu entre flexibilité et contrôle dans la conception de leurs rôles.
> L'entreprise a décidé de créer des rôles plus petits, basés sur des fonctions ou des tâches (par exemple, le traitement des bons de commande) afin de fournir le degré de flexibilité nécessaire.

La méthode de dérivation a été rejetée en raison du grand nombre de rôles qu'elle aurait généré, compte tenu du nombre de valeurs associées aux domaines de contrôle (codes entreprise ou usines, etc.). Plus récemment la méthodologie choisie pour la définition de rôles techniques et opérationnels reposait sur la tâche et la valeur.

En fonction des types de rôles, le projet s'organisait comme suit:

- *Rôles utilisateurs finaux opérationnels :* À l'aide des journaux de transactions utilisateurs (SM20), les rôles définis via des tâches ont été attribués aux utilisateurs sur la base des données historiques, sous réserve de la validation du supérieur hiérarchique direct. Plusieurs rôles fonctionnels ont été identifiés et appliqués comme rôles opérationnels. Cela permet de faciliter les modifications en cas de besoin. Un accès au niveau organisationnel a été fourni grâce aux rôles définis via des valeurs.
- *Rôles techniques (Phase 1) :* Les rôles définis de manière appropriée via des tâches et associés à des fonctions techniques (par ex. fondamentaux, administration des autorisations, etc.) ont limité le risque d'accès trop larges octroyés aux équipes d'assistance internes et aux prestataires externes.
- *Rôles techniques (Phase 2) :* Restriction des objets d'autorisations critiques fondamentaux, avec une attention particulière à la mise en place d'un accès RFC (Remote Function Call) détaillé.

Personnalisation des ensembles de règles

Les ensembles de règles regroupent des règles liées aux risques GRC identifiés. Ils sont créés dans le but de relier les contrôles d'atténuation aux risques associés aux processus métier. L'ensemble de règles standard mis au point par Soterion a dû être adapté pour répondre aux besoins spécifiques de Saint-Gobain. Lors de sa mise en œuvre, la solution Soterion a été accompagnée d'un ensemble de règles dédié aux risques d'accès leader sur le marché. Néanmoins, comme tout autre ensemble de règles standard ou prêt à l'emploi, il est conçu pour être appliqué aux entreprises, indépendamment du secteur d'activité et de l'implantation géographique. Établir un ensemble de règles sur mesure pour Saint-Gobain Afrique du Sud a été une étape importante du parcours afin de garantir l'adhésion de l'entreprise.

Atténuation

Puisqu'il est impossible d'obtenir un risque zéro en matière d'accès, les mesures d'atténuation jouent un rôle vital pour limiter l'exposition au risque du client. Il était important de réduire ces risques, à la fois inévitables et en lien avec l'entreprise. De nombreuses mesures existaient déjà dans cette entité. Ces contrôles ont été identifiés et documentés dans un répertoire central, puis cartographiés en fonction des risques dans l'ensemble de règles personnalisé.

Formation professionnelle

Une partie de la solution a consisté à former les responsables hiérarchiques directs au sujet des risques et des contrôles d'atténuation qui relèvent de leur périmètre afin de favoriser la prise de responsabilité. Les chefs d'unités opérationnelles ont été formés pour comprendre le contenu de leurs vérifications afin qu'ils puissent prendre des décisions éclairées. Cela s'est également traduit par une meilleure conscience du risque au sein de l'entreprise.

Gestion des accès d'urgence

Dans certaines circonstances, les utilisateurs issus des métiers ou des services d'assistance avaient besoin d'un accès temporaire ou ponctuel (d'urgence) pour mener des activités essentielles à l'entreprise. Saint-Gobain Afrique du Sud a confié la gestion de ses accès sensibles et d'urgence au gestionnaire des droits avancés de Soterion. En cas de besoin, ce module permet aux services d'assistance comme aux équipes métier d'accéder aux fonctions sensibles de façon contrôlée. Les sessions de droits avancés sont sauvegardées et leur activité est envoyée aux propriétaires pour examen.

La suite de l'aventure : les prochaines étapes pour Saint-Gobain Afrique du Sud

L'adoption d'une gestion GRC efficace est un processus continu. Chaque parcours GRC a pour but de mettre en place une gestion flexible et effectivement contrôlée des droits d'accès utilisateurs.

Pour Saint-Gobain Afrique du Sud, les prochaines étapes consistent en :

- l'examen des accès utilisateurs : Mise en œuvre d'une procédure de demande, révision et validation des accès.
- la gestion des identités : pour parfaire son minutieux contrôle d'accès, Saint-Gobain Afrique du Sud envisagera l'acquisition d'une solution de gestion des accès et des identités.

L'infogérance au service de la GRC

Plus que de la sous-traitance

Un système SAP évolue continuellement au même rythme que l'entreprise qui l'accueille. Des collaborateurs changent de service, des recrues sont intégrées et, dans le cas de groupes de sociétés, des mutations ont lieu vers des filiales. Il est nécessaire d'ajuster les accès utilisateurs à chaque changement mais sans une assistance appropriée, les collaborateurs conservent souvent des droits inadaptés. Outre sa volonté de maintenir la solution en bon état, l'entité sud-africaine de Saint-Gobain comprend les enjeux de ses autorisations SAP et les place en priorité par rapport à son parcours GRC. Elle sait que l'intégrité de son système d'autorisation repose en grande partie sur la capacité de son prestataire externe à mettre en œuvre des bonnes pratiques en accord avec sa nouvelle approche. Compte tenu des mauvaises expériences rencontrées auprès d'anciens sous-traitants, il apparait évident que l'entreprise ne veut pas simplement externaliser ses autorisations. Au contraire, elle cherche même une offre plus complète : l'infogérance au service de la GRC.

Comment fonctionne la GRC en infogérance ?

La GRC en infogérance repose sur une relation entre le prestataire et le client qui allie expertise et technologie en vue de satisfaire certains besoins. Il ne s'agit pas simplement d'externaliser des activités techniques, mais de construire un partenariat où le prestataire de services s'occupe du client comme s'il faisait partie de l'entreprise. Dans le cadre de la GRC de SAP, l'infogérance va plus loin que les autorisations SAP classiques et inclut un service d'assistance en matière de risque, de contrôles et d'audit. À mesure que Saint-Gobain Afrique du Sud affine son parcours GRC, le savoir-faire de ses équipes lui permet d'internaliser certaines des activités. Ainsi, l'entreprise ne dépend plus totalement de l'assistance du prestataire externe pour effectuer les opérations liées aux autorisations. Désormais, l'attribution des rôles est gérée en interne, seule la modification du contenu des rôles a besoin d'être externalisée. Dans le cadre de ce développement, Saint-Gobain Afrique du Sud a créé un service dédié aux contrôles en interne. Cela a permis de transférer la responsabilité des équipes informatiques aux opérationnels, permettant ainsi aux créateurs de processus de mieux connaître les risques associés à leur domaine et, donc, de mieux les contrôler.

> L'un des enjeux permanents de Saint-Gobain Afrique du Sud était les contrôles d'accès à ses systèmes SAP. Le risque lié aux accès n'était pas clairement mesuré et les glissements d'autorisation étaient fréquents. Les problèmes rencontrés se sont aggravés du fait des prestataires externes qui, au lieu de guider les équipes pour adopter de meilleures pratiques, effectuaient des opérations techniques sur demande. À terme, au fil des changements de prestataires, la multiplication des méthodologies de création des rôles a largement compliqué la gestion des accès. Tous ces problèmes se reflétaient dans les résultats des audits surprise, souvent infructueux. Du fait de sa collaboration avec Soterion, Saint-Gobain Afrique du Sud a adopté une nouvelle définition des rôles qui lui a permis de mener à bien ses audits. Grâce à une meilleure compréhension des risques métier et à un contrôle des accès plus poussé, les propriétaires de processus métier ont gagné en responsabilité dans leur domaine. Grâce à la solution Soterion, les chefs d'unités opérationnelles bénéficient de plus de visibilité, d'un meilleur contrôle et de l'adhésion des cadres. La GRC (gouvernance, risque et conformité) constitue un engagement continu.Avec l'appui de Soterion, Saint-Gobain Afrique du Sud s'est muni d'une base solide pour ses autorisations et d'un plan d'action clair pour la suite.