

Gestion de la gouvernance, des risques et de la conformité : **VERS DE NOUVELLES ALTERNATIVES EN EUROPE**

L'importance des solutions de gestion de la gouvernance, des risques et de la conformité (GRC) pour les ERP, n'est plus à démontrer. Les scandales financiers Enron, Tyco International ou encore WorldCom, qui ont éclaté dans les années 2000 ont fait le travail de sensibilisation des entreprises, accentué par la mise en application des lois Sarbanes Oxley et de Sécurité Financière. Il en résulte aujourd'hui un niveau de maturité assez avancé de la part des entreprises du CAC40.

ControlPanel[®] GRC

PAR MEHDI KEFI, RESPONSABLE DE L'OFFRE GRC CHEZ HARMONIE TECHNOLOGIE

Si les DSI sont désormais convaincus de l'importance de l'approche GRC, c'est la gestion du risque et non plus la conformité qui les incite à investir dans les solutions disponibles. La conformité est devenue un prérequis. « *Mais le grand défi, avec la majorité des solutions GRC, a toujours été leur morcellement, leur complexité, leur cherté, et le temps de les mettre en œuvre.* » déclare Mehdi Kefi, Senior Manager GRC chez Harmonie Technologie. C'est pourquoi, Harmonie Technologie annonce son partenariat GRC avec Symmetry pour couvrir les risques opérationnels dans les systèmes SAP. « *Nous pouvons dès lors proposer une alternative avec une plate-forme de gouvernance, de gestion des risques et de conformité (GRC) puissante, flexible, simple à mettre en place. Cette solution permet de réaliser des économies de temps et de coûts considérables en automatisant les tâches de conformité et d'audit.* » ajoute Mehdi Kefi.

LES ENJEUX GRC SUR LE MARCHÉ FRANÇAIS

Le niveau d'adoption de solutions GRC est porté par 2 facteurs : la pression des investisseurs et la pression réglementaire. Les investisseurs expriment un besoin fort en conformité mais aussi en gestion des risques, de manière à instaurer la confiance auprès des clients. Depuis les lois Sarbanes Oxley et de Sécurité Financière, la législation s'est renforcée en matière de contrôle interne et de protection des données : ISO, Bâle III, Sapin 2 et plus récemment RGPD et NIS. De plus, les commissaires aux comptes, les auditeurs externes et les équipes d'audit interne étudient de près les risques opérationnels et exigent que l'entreprise s'aligne aux bonnes pratiques de contrôle interne.

COMMENT FAIRE ÉVOLUER SON NIVEAU DE MATURITÉ ?

Le niveau de maturité GRC des entreprises en France est assez élevé. On distingue 4 niveaux de maturité :

1. Le premier niveau concerne toute entreprise qui n'a peu ou pas encore défini des processus de gestion des droits d'accès et est contrainte d'adopter une posture « réactive ».
2. L'entreprise atteint un second niveau de maturité lorsqu'elle met en place un dispositif de contrôles pour anticiper ses risques. Ce plan inclut la formalisation et l'automatisation des processus de gestion des droits d'accès.
3. Le troisième niveau est atteint, lorsqu'elle adopte une posture « préventive » en connaissant son exposition aux risques, à tout moment, avec un plan de contrôles qui priorise les actions et qui est validé régulièrement.
4. Enfin, elle acquiert un dernier niveau de maturité « efficient », lorsque qu'elle coordonne l'analyse et l'action, adhère aux objectifs de l'entreprise et se dote d'une vision globale aux risques, à l'exposition et à la performance.

La plupart des entreprises du CAC40 ont atteint les niveaux 2 ou 3. En revanche, les entreprises du middle-market sont en retard sur ce sujet avec au mieux, dans la grande majorité des cas, une solution de gestion des droits d'accès (niveau 2). « *La sécurité des données et le renforcement du contrôle interne sont nettement améliorés par l'alignement des rôles avec les besoins métiers et la mise en place de la séparation des tâches. Mais ces mesures permettent surtout d'améliorer la performance opérationnelle en facilitant les réorganisations et en clarifiant les périmètres de responsabilités des fonctions supports.* » précise Mehdi Kefi.

« Avec d'un côté les exigences du RGPD et de l'autre un nombre croissant de clients cherchant à moderniser et faire migrer leurs environnements SAP, beaucoup d'entreprises commencent à regarder de plus près leurs processus de contrôle des accès et de séparation des tâches, pour s'assurer de leur conformité et être prêtes pour les audits. » explique Scott Goolik, vice-président Conformité et sécurité chez Symmetry.

Plus riche en fonctionnalités et moins couteuse, la solution ControlPanelGRC® de Symmetry, encore peu connue en France, pourrait séduire de grands groupes ainsi que les entreprises du middle-market à l'image de l'industriel, TIRU, filiale de Dalkia au sein du groupe EDF, qui vient de franchir le pas et signe la première référence ControlPanelGRC® sur le territoire français.

GÉRER ET RÉDUIRE SES RISQUES OPÉRATIONNELS DANS SAP

TIRU, entreprise de pointe dans le secteur de la valorisation énergétique des déchets, a souhaité refondre l'ensemble des droits d'accès dans SAP, pour se conformer aux exigences de séparation des tâches et pour réaligner les autorisations SAP avec les derniers changements organisationnels du groupe. Dès lors, pour l'accompagner dans cette transformation, elle a sollicité Harmonie Technologie, cabinet de conseil, français, indépendant, spécialiste de la cybersécurité et de la gestion des risques, pour lui trouver la solution la plus adaptée à son besoin. Ce projet, étalé sur 8 mois, concerne les 17 sites de TIRU, représentant en tout 400 utilisateurs. « Nous avons proposé ControlPanelGRC® de Symmetry, le spécialiste américain de la gestion des applications d'entreprise, de l'hébergement cloud hybride et des solutions GRC qui présente des coûts plus bas que SAP et des avantages techniques éprouvés. ControlPanelGRC® apporte en effet une valeur ajoutée à nos clients qui recherchent une alter-

native plus économique et plus efficace pour gérer les risques SoD, les comptes à pouvoir, les plans de contrôles compensatoires ou encore le provisioning des utilisateurs. » précise Mehdi Kefi et de poursuivre « en établissant un budget prévisionnel pour TIRU, dès la première année, ControlPanelGRC® est moins cher que SAP GRC Access Control, et nécessite un faible coût de maintenance. Par ailleurs, ControlPanelGRC® est complètement intégré dans SAP. Il n'est donc pas nécessaire d'avoir un serveur dédié et interfacé aux systèmes SAP (développement, production, voire Q&A). ControlPanelGRC® démontre enfin une meilleure flexibilité pour s'adapter aux besoins du client. »

Après un cadrage en fin d'année 2017, l'objectif de mise en production fixé en juillet dernier a été respecté. L'ensemble des rôles ont été refondus, toutes les fiches métiers ont été documentées et l'ensemble des risques a été soit éliminé, soit mis sous contrôle à l'aide de plans d'actions dédiés. « Harmonie Technologie nous a soutenu du début à la fin pour l'intégration de ControlPanelGRC® de Symmetry, pour la refonte de nos rôles SAP et pour la remédiation des risques SoD. J'ai particulièrement apprécié la double compétence technique et fonctionnelle de l'équipe d'Harmonie Technologie. Outre le travail de qualité qui a été accompli, ils ont donné aux gestionnaires de domaines et aux responsables de sites les outils nécessaires pour collaborer – ce qui a grandement facilité l'adoption du projet. » déclare Véronique Chamard, à la tête du service informatique de TIRU. « Nous sommes ravis que la solution tienne ses promesses initiales, qui étaient une intégration rapide et une personnalisation simple. Nous n'avons pas seulement gagné en sécurité et en efficacité pour ce qui est d'identifier les risques SoD et leur résolution, nous avons également automatisé et sécurisé les processus de création et de modification de nouveaux rôles – composés, dérivés ou parents. »

TIRU illustre parfaitement la facilité et la rapidité de mise en œuvre et d'utilisation de ControlPanelGRC®.

« TIRU illustre parfaitement la facilité et la rapidité de mise en œuvre et d'utilisation de ControlPanelGRC® – en particulier pour les utilisateurs dans ces entreprises. Nous sommes impatients de collaborer avec Harmonie Technologie sur d'autres engagements clients et de développer nos opérations sur le marché européen. » ajoute Scott Goolik, vice-président Conformité et sécurité chez Symmetry.

CONTROLPANELGRC®

40% des clients de Symmetry ont migré de SAP GRC Access Control vers la solution ControlPanelGRC® notamment pour la mise à disposition de fonctionnalités plus nombreuses et couvrant un périmètre plus large :

- Gestion du cycle de vie des rôles améliorée, rôles parents et dérivés
- Notions de famille et restriction organisationnelles bien définies
- Mise en place facile des workflows pour le suivi des contrôles compensatoires
- Reporting très riche
- Identification des risques potentiels, avérés et réels
- Consultation de rapports immédiatement exploitables pour analyser les risques dans le détail
- Outils d'aide à la décision plus efficaces
- Changement possible de mot de passe par l'utilisateur
- Gestion des licences, des clés de modification et de réparation.