Evaluation des tiers

Il est temps de mettre en œuvre une gestion des risques à 360°

protiviti®
Face the Future with Confidence

Mai 2018

L'accélération du rythme des règlementations et des programmes de conformité a mis en lumière l'élargissement du concept d'entreprise au-delà de ses murs. Que ce soit d'un point de vue corruption (loi « Sapin 2 » du 9 décembre 2016), devoir de vigilance (loi du 27 mars 2017) ou bien RGPD (règlement européen en vigueur à partir du 25 mai 2018), ces règlementations imposent avec plus ou moins de fermeté des diligences à mettre en œuvre par les entreprises vis-à-vis de ses tiers, et notamment ses fournisseurs.

Les fonctions achats d'ores et déjà à l'œuvre en matière de gestion des risques fournisseurs… parfois au contraire des directions de la conformité

La gestion des risques fournisseurs évolue rapidement depuis quelques années. Historiquement centrée sur des natures de risques opérationnelles et spécifiques (gestion de la qualité, gestion de la résilience et de la continuité d'activité en cas de crise, contrôle interne des prestations externalisées – ISAE 3402, dépendance du fournisseur à la relation d'affaires, robustesse financière, etc.), l'univers de risques auxquels les tiers sont susceptibles d'exposer la société se doit d'intégrer également des problématiques d'éthique et de conduite des affaires (ex : sanctions / embargos et contrôle des exportations).

Les fonctions achats ont donc d'ores et déjà du mettre en œuvre des politiques et procédures opérationnelles depuis plusieurs années afin d'intégrer la gestion de ces risques au sein de leur processus opérationnels de qualification, de « sourcing » et de contractualisation, puis de suivi de la relation d'affaires.

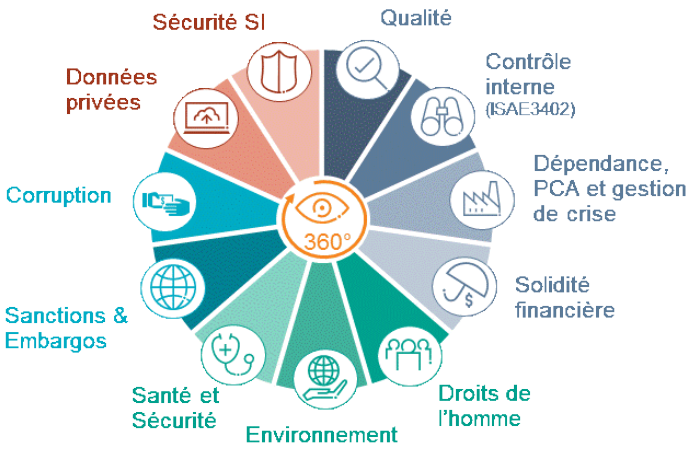

Fig. 1 : Exemple « d'univers de risques » liés aux tiers

Nous pouvons toutefois noter que les fonctions achats avaient jusqu'à présent un éventail d'interlocuteurs variés au sein de l'entreprise (finance, qualité, etc.) favorisant des démarches en silo ainsi qu'un manque d'homogénéité et de coordination. Nous constatons par ailleurs trop souvent un manque d'implication opérationnelle des fonctions conformité sur ces processus d'évaluation et de qualification des fournisseurs, et ce, malgré la criticité des risques intrinsèques auxquels ils exposent l'organisation.

Sapin 2, Devoir de vigilance et RGPD : une superposition de nouvelles couches qui rend nécessaire une refonte et une harmonisation des démarches d'évaluation des risques fournisseurs

Une nouvelle vague de règlementations (Sapin 2, Devoir de vigilance, RGPD) ajoute une couche supplémentaire à la superposition de l'ensemble des mesures de gestion des risques de tiers qui peut devenir difficilement supportable au niveau opérationnel sans repenser une véritable gestion des risques à 360°.

Le temps est ainsi venu de coordonner et d'harmoniser ces démarches pour les rendre plus efficaces et pérennes. L'ensemble de ces démarches s'appuient opérationnellement sur des fondamentaux méthodologiques identiques.

Prenons l'exemple de ces trois règlementations qui occupent plus particulièrement les directions de conformité depuis plusieurs mois : Sapin 2, Devoir de vigilance et RGPD.

1. Premièrement, l'approche à mettre en œuvre pour ces règlementations nécessite une catégorisation systématique des biens et/ou des typologies de services achetés, des données transférées (et donc des catégories de fournisseurs associés) et ce, selon l'exposition au risque concerné. Directement dérivées d'une approche par les risques ou d'une cartographie des risques de non-conformité (cartographie des risques vigilance, cartographie des risques de corruption, cartographie des données privées et des traitements associés), ces classifications de produits/services/données vont permettre de déterminer le périmètre des tiers à prendre en compte dans la démarche, et la nature de risque associée.
2. Ensuite, il est nécessaire de déterminer une méthodologie de cotation de chaque nature de risque. Cette notation ou « scoring » peut reposer sur plusieurs critères en fonction des natures de risques auxquels le tiers expose l'organisation (la catégorie intrinsèque du tiers, la nature des biens/services achetées ou des données traitées, le pays dans lequel il opère, sa structure juridique et ses bénéficiaires effectifs, etc.)
3. Cette notation du risque associé à chaque famille de produits/services/données et typologies de fournisseurs va ensuite conditionner le niveau de vérifications et de contrôles à effectuer à chaque stade de la relation, comme par exemple :
   - Le niveau de diligences (questionnaire, base externe, enquête) avant l'entrée en relation,
   - La nature des clauses contractuelles,
   - L'adhésion au principes du code de conduite de la société,
   - Les modalités de surveillance de la relation d'affaire (audit réguliers, vérifications à chaque commande / à chaque paiement) et la mise en place d'un suivi plus ou moins régulier et rapproché,
   - La fréquence d'actualisation des données du fournisseur et de son dossier de risque, etc.
4. Enfin, et ce point est souvent sous-estimé dans les projets, la gestion de l'historique relève souvent du casse-tête. Il s'agit de traiter les relations existantes en définissant des priorités, en appliquant la méthodologie ci-dessus vis-à-vis des partenaires historiques tout en prenant en compte les contrats commerciaux en cours.

LES POINTS CLES D'UNE APPROCHE DES GESTION DES RISQUES DE TIERS

SCOPING	La phase de « scoping » permet de déterminer les catégories de tiers à inclure dans la démarche et les natures de risques auxquels ils peuvent exposer l'organisation
SCORING	La phase de « scoring » permet d'affecter une notation du tiers en fonction de son profil de risques
ENTREE EN RELATION	Sur la base de la notation, des niveaux de diligences différenciées peuvent être effectuées avant l'entrée en relation sur les différentes natures de risque
SUIVI DE LA RELATION	Une fois l'entrée en relation effectuée, le suivi de la relation d'affaires s'effectue également en fonction de la notation du tiers (ainsi que son actualisation dans la durée)

Contacts

Bernard Drui, Managing Director | bernard.drui@protiviti.fr

Arnaud Floquet, Managing Director | arnaud.floquet@protiviti.fr

Silvia Nanni Costa, Director | silvia.nannicosta@protiviti.fr