Deloitte.

À l'ordre du jour du conseil | Mai 2016

Dans ce numéro...

Nous sommes heureux de vous présenter *À l'ordre du jour du conseil*, une publication qui traite de questions d'actualité pertinentes pour les administrateurs. Chaque numéro traite en détail d'un sujet et présente le point de vue d'un professionnel de Deloitte ayant une connaissance approfondie de la question ainsi que celui d'un administrateur externe d'expérience.

Chantal Rassart
Associée, Centre canadien de gouvernance d'entreprise

Michael Rossen
Directeur de service, Centre mondial de gouvernance d'entreprise

Gestion du risque de l'entreprise étendue

Le risque lié aux entités tierces

L'usine d'un fournisseur s'effondre, faisant des centaines de victimes parmi les travailleurs, dont certains sont des enfants. Des milliers de fichiers contenant des données sur les cartes de crédit de clients et d'autres renseignements financiers confidentiels font l'objet de piratage d'un tiers autorisé à accéder au réseau de l'entreprise. Un fournisseur a utilisé des matériaux contaminés et une vaste campagne de rappel visant certains produits doit être lancée.

Encore récemment, le risque lié aux fournisseurs se limitait pour ainsi dire à la qualité des produits ou des matières premières fournis ou à la possibilité qu'un fournisseur ne respecte pas ses engagements d'approvisionnement et perturbe ainsi la production.

De nos jours, des lois comme la Foreign Corrupt Practices Act aux États-Unis, la Bribery Act au Royaume-Uni et d'autres encore font en sorte que les entreprises sont de plus en plus souvent tenues responsables des agissements de leurs fournisseurs. De même, les clients ne distinguent pas toujours une entreprise de ses fournisseurs. Pour eux, l'entreprise est celle qui leur fournit une solution; s'il survient un problème, c'est elle qu'ils tiennent responsable, et c'est donc sa réputation qui est en péril. C'est pourquoi les entreprises doivent maintenant élargir leur surveillance des risques à l'entreprise étendue[1] et observer chez leurs tiers fournisseurs les pratiques de santé, de sécurité et d'environnement, le respect des lois sur le travail et autres règlements, l'utilisation de la propriété intellectuelle, l'approvisionnement en matières premières, la corruption et plus encore.

> L'un des enjeux les plus importants pour les entreprises consiste à bien comprendre l'envergure exacte de leurs relations avec des tiers et les risques qui s'y rattachent.

[1]Dans le contexte de la mondialisation, aucune entreprise ne fait cavalier seul. L'écosystème d'une entreprise type comprend un nombre grandissant d'entités avec lesquelles l'entreprise interagit : ses clients, ses partenaires commerciaux, ses agents, ses affiliés, ses fournisseurs et ses fournisseurs de services. Ensemble, ces entités tierces représentent l'« entreprise étendue ».

C'est ainsi que le risque lié aux entités tierces figure de plus en plus souvent à l'ordre du jour des conseils d'administration. D'après un récent sondage mené par Deloitte, à l'échelle mondiale, 87 % des 170 entreprises sondées ont dû faire face à un incident perturbateur impliquant des tiers dans les deux ou trois dernières années. Le sondage a également révélé que les gestionnaires admettent de plus en plus la nécessité de resserrer la responsabilité de la gestion du risque lié aux tiers au niveau des administrateurs et des cadres supérieurs de manière à relier explicitement le risque et la stratégie et à exploiter au mieux les possibilités de l'écosystème formé par des entités tierces[2].

L'entreprise étendue

L'un des enjeux les plus importants pour les entreprises et leurs administrateurs consiste à bien comprendre l'envergure exacte de leurs relations avec des tiers et les risques qui s'y rattachent.

Les grandes sociétés, notamment, entretiennent des milliers de ces relations et perdent souvent de vue la portée complète de leur entreprise étendue. L'écosystème de la plupart des entreprises comprend des tiers de deuxième, voire de troisième niveau, dont les entreprises sont parfois entièrement inconscientes et dont les actions peuvent néanmoins se répercuter sur elles et entacher leur réputation. Les tiers sont parfois situés à l'étranger, où ils obéissent à des normes et à des pratiques commerciales ou culturelles qui leur sont propres, ce qui complique leur supervision et la surveillance de leurs méthodes.

Les administrateurs doivent s'assurer que l'entreprise a déjà déterminé à quels risques les tiers et leurs activités sont susceptibles de l'exposer. L'entreprise doit donc acquérir une vision d'ensemble de son risque lié aux tiers; elle doit pouvoir déterminer s'il existe une concentration de ce risque sur le plan des fournisseurs, des produits, des marchandises, des régions géographiques ou d'autres paramètres. Là où la concentration est importante, l'entreprise doit s'astreindre à une diversification de ses relations avec des tiers.

Gestion du risque

Toute entreprise doit cerner les composantes du risque de son entreprise étendue susceptibles d'aggraver la vulnérabilité de son organisation. Les administrateurs doivent s'assurer que la direction tient compte du risque lié aux tiers dans son appréciation globale des risques et que des mesures suffisantes sont mises en application, au niveau du conseil comme au niveau de l'équipe de direction, pour que l'entreprise puisse gérer toutes les composantes du risque de sa chaîne de valeur et soit munie des contre-mesures nécessaires pour faire face à tout problème soulevé par une relation avec un tiers. Une façon de faire consiste à vérifier que l'entreprise possède une couverture d'assurance suffisante pour se protéger en cas de défection majeure d'un tiers.

Si elles tiennent maintenant compte d'un faisceau plus large de risques liés aux tiers qu'auparavant, c'est au chapitre des méthodes de gestion de ces risques que les entreprises doivent encore faire des progrès. Certaines entreprises, par exemple, s'en remettent toujours à une méthode axée sur la gestion des contrats, estimant que la diligence raisonnable mise en œuvre avant la signature suffit à réduire les risques associés à la contrepartie au contrat. Aucune autre évaluation des risques n'est alors effectuée : l'entreprise adopte une approche réactive à la gestion du risque lié aux tiers, et bien souvent les problèmes ne sont découverts et pris en charge qu'après coup, quand ils ont eu lieu et que le dommage est fait.

Une autre façon de faire consiste à dresser une liste des fournisseurs de prédilection. Rares sont cependant les entreprises qui vont jusqu'à attribuer une cote de risque aux fournisseurs de la liste, c'est-à-dire à cerner ceux dont les activités ont été inspectées et jugées de qualité supérieure, à les distinguer de ceux qui méritent d'être surveillés de plus près et, enfin, à isoler ceux avec lesquels l'entreprise ne souhaite pas nouer de relation.

Une gestion proactive de ces tiers suppose que l'entreprise définisse ses normes et ses attentes à l'égard des principales pratiques auxquelles ses fournisseurs devraient adhérer selon elle. L'entreprise devrait aussi formuler des dispositions contractuelles décrivant les validations, le suivi, les mises à l'essai et les autres mesures de vérification auxquelles elle aura recours pour s'assurer que ses fournisseurs respectent bel et bien les normes définies. Elle peut par exemple demander aux fournisseurs de réitérer annuellement leur engagement à respecter les valeurs essentielles de l'entreprise ou se réserver le droit de visiter les installations de ses fournisseurs pour examiner sur place les pratiques de ces derniers. Toute entente conclue avec un tiers devrait stipuler sans équivoque que le non-respect des normes de l'entreprise entraînera la résiliation du contrat ou une autre mesure punitive.

Bien que nombre d'entreprises fassent affaire avec des tiers situés à l'étranger où la réglementation, les pratiques commerciales et les normes déontologiques ne sont pas nécessairement les mêmes, les activités des tiers faisant partie de leur entreprise étendue sont de plus en plus souvent jugées en fonction des normes en vigueur dans le territoire dont elles sont elles-mêmes originaires. Il est donc normal que les entreprises imposent leurs valeurs à leur entreprise étendue. Cependant, elles doivent garder à l'esprit que toutes leurs pratiques ne sont pas directement pertinentes pour un tiers donné, et qu'une adaptation au contexte local est parfois nécessaire. L'établissement de bons canaux de communication bilatéraux avec les membres de l'entreprise étendue favorise l'adhésion de ces derniers aux normes et aux valeurs de l'entreprise.

[2]Deloitte, *Third party governance and risk management: The threats are real,* 2016.

Timothy Scott
Associé, Service des risques d'entreprise
Deloitte Canada

Timothy Scott est associé au Service des risques d'entreprise de Deloitte, au Canada. Il compte plus de 23 ans d'expérience, tant auprès de cabinets de services professionnels que d'entreprises du secteur, et se spécialise dans l'évaluation des risques liés aux tiers et de leur rendement, de l'audit interne et de la gestion du risque d'entreprise.

Chez Deloitte, M. Scott dirige le service national Gestion des risques liés aux tiers et Conformité, fournissant aux clients des services relatifs aux évaluations des risques liés aux tiers et de leur rendement, aux évaluations de la conformité et du rendement des franchises, à la gestion des biens logiciels, aux accords de licence et de redevance, et aux dépenses en immobilisations.

Mark Victor
Associé, Gouvernance, risque et conformité
Deloitte Afrique du Sud

Mark Victor est directeur de service au sein des Services-conseils en gestion des risques chez Deloitte en Afrique du Sud. Il s'agit d'une équipe intégrée d'experts en matière de gouvernance, de gestion du risque, de conformité réglementaire et de contrôles, fournissant une vaste gamme de services-conseils financiers spécialisés aux institutions financières et aux entités du secteur public de l'Afrique australe. L'expérience particulière de M. Victor comprend les services-conseils auprès de banques, de sociétés d'assurance, de caisses de retraite et de services médicaux.

Il a de l'expérience dans la prestation de services-conseils en matière de gouvernance d'entreprise, de réglementation et de risque. Il a conseillé des clients en ce qui concerne l'adoption de pratiques exemplaires de gestion du risque. M. Victor possède aussi une expérience approfondie de la prestation de services d'audit interne impartis à des fonctions d'audit interne dans un large éventail de secteurs, et de services-conseils en matière de réglementation, de gestion des risques, de gouvernance et de conformité.

« L'un des plus gros risques qui guettent une entreprise, c'est la méconnaissance de son entreprise étendue. Le conseil d'administration doit veiller à ce que l'entreprise se protège contre ce risque en dressant l'inventaire complet de ses entités tierces et en supervisant la mise en place des contrôles et processus de gestion proactive. L'objectif est de réduire le risque lié aux tiers en améliorant la qualité et la fiabilité des relations entretenues avec eux. »

Questions que les administrateurs devraient poser

1. Notre entreprise a-t-elle évalué de manière exhaustive son risque lié aux tiers et, si c'est le cas, quelles en sont les composantes les plus déterminantes pour l'entreprise à l'heure actuelle?

2. Quels sont les tiers susceptibles d'entraver le plus gravement la capacité de l'entreprise à atteindre ses buts et objectifs stratégiques?

3. Que faisons-nous pour gérer et surveiller de manière proactive le risque et son évolution au sein de notre entreprise étendue? Quels outils de gestion du risque utilisons-nous?

4. Qui est responsable de la gestion du risque lié aux tiers dans notre entreprise?

5. À quelle fréquence la direction informe-t-elle le conseil d'administration de son évaluation des risques de tiers et du processus mis en place pour atténuer ces risques? Cette information est-elle suffisamment détaillée et présentée en temps opportun?

Point de vue d'un administrateur

José Écio Pereira est membre des conseils d'administration de Votorantim Cimentos, Fibria et Gafisa et a été membre du conseil de BRMalls; il préside également le comité d'audit de Votorantim Cimentos et de Gafisa. Il est le propriétaire fondateur de JEPereira Consultoria em Gestão de Negócios et a été associé, maintenant à la retraite, de Deloitte Brésil.

Le risque lié aux entités tierces figure-t-il à l'ordre du jour des conseils d'administration?
Les conseils dont je connais le fonctionnement effectuent une évaluation du risque tous les trois ou quatre mois. Le risque lié aux entités tierces à proprement parler n'est pas un point distinct à l'ordre du jour, mais nous l'abordons dans notre analyse des risques. Ceci dit, il est clair que de nos jours, les conseils accordent plus d'attention au risque lié aux tiers qu'il y a à peine deux ans. Au Brésil, c'est principalement à cause de la loi anticorruption (Clean Company Act) de 2014. En vertu de cette loi, les entreprises peuvent être tenues responsables des activités illégales ou de la conduite contraire à l'éthique de leurs tiers fournisseurs.

Depuis que cette loi est en vigueur, les administrateurs examinent de beaucoup plus près les risques associés aux tiers fournisseurs des entreprises qu'ils supervisent. Ils examinent les pratiques de leurs fournisseurs en matière de conditions de travail, de normes pour les employés, de mesures de santé et de sécurité et d'autres facteurs pour s'assurer que tous respectent les normes de l'entreprise qui a fait appel à eux. La santé financière des fournisseurs est un autre paramètre fort important, surtout au vu de la situation économique actuelle au Brésil. Les entreprises veulent être sûres que leurs fournisseurs paient leurs impôts et respectent leurs obligations juridiques, en particulier dans leurs relations avec leurs employés, et qu'ils seront à même de poursuivre leur exploitation.

Les administrateurs examinent-ils les relations avec des tiers dans le contexte du cyberrisque?
Je pense que les entreprises dont les systèmes sont connectés avec ceux de tiers fournisseurs à des fins d'approvisionnement ou de logistique sont conscientes de l'existence du cyberrisque et prennent les mesures nécessaires pour s'en prémunir. Mais ces mesures sont généralement liées aux échanges de produits et de services.

Dans une perspective plus vaste, je dirais que la plupart des entreprises ne disposent pas de systèmes d'information appropriés pour gérer leurs relations avec des tiers. Les systèmes de la plupart des entreprises ne sont pas assez sophistiqués pour se connecter aux systèmes des fournisseurs; les entreprises ont recours à divers outils pour gérer leurs relations avec des tiers et souvent, ces outils ne sont pas très bien intégrés entre eux. Les relations sont par exemple gérées à l'aide de plusieurs systèmes, y compris des chiffriers et des outils manuels qui ne sont pas du tout conçus pour cet usage.

À qui devrait revenir la responsabilité des tiers fournisseurs?
Le conseil d'administration doit jouer un rôle de supervision et faire en sorte que les cadres supérieurs disposent d'un processus de gestion du risque lié aux tiers.

Au Brésil, c'est souvent le service de l'approvisionnement qui reste responsable des problèmes opérationnels et qui vérifie que les produits et les services sont bien fournis selon les modalités du contrat conclu avec le tiers fournisseur. De plus, nombre d'entreprises mettent aussi sur pied une fonction particulière chargée de la gestion des contrats conclus avec des tiers. La plupart des entreprises brésiliennes entretiennent plusieurs relations avec des tiers : services alimentaires, sécurité, transports, fabrication. Toutes sont essentielles au fonctionnement d'une entreprise au quotidien. Les entreprises sont donc nombreuses à affecter davantage de ressources à la gestion efficace des contrats.

Certaines entreprises surveillent constamment leurs fournisseurs pour s'assurer que les contrats sont observés à la lettre. Bon nombre exigent que leurs fournisseurs autoévaluent leur conformité contractuelle, en plus d'effectuer des audits périodiques et d'autres tests afin de vérifier le respect des contrats. Toutes ces mesures représentent un travail colossal et parfois, il faut y consacrer une fonction administrative particulière.

Je vais vous relater un exemple authentique. L'une des sociétés avec lesquelles je collabore est en train de construire de nouvelles installations de grande envergure. C'est un investissement de près de 2 milliards de dollars américains, et c'est un projet d'environ : 18 mois. À l'heure actuelle, la construction vient juste de commencer. Plusieurs fournisseurs y travaillent, que ce soit pour la sécurité du chantier ou pour l'approvisionnement en matériel ou son installation.

L'entreprise a mis sur pied un comité directeur de projet qui comprend entre autres des membres de l'équipe de direction. Ce comité se réunit au moins une fois tous les : 15 jours, et les relations avec les fournisseurs reviennent justement sans cesse à son ordre du jour. C'est beaucoup plus qu'une question de diligence raisonnable; le comité procède aussi au suivi constant des tiers fournisseurs.

Le comité directeur présente chaque mois au conseil l'état d'avancement du projet. Le rapport d'avancement consigne tout ce qui a trait aux tiers fournisseurs : le défaut de verser les retenues sur salaires des employés, de payer des impôts fonciers ou des avantages sociaux, la violation des règles de santé et de sécurité sur le chantier, aussi bien que les problèmes opérationnels comme le non-respect des échéances par un fournisseur ou la qualité insuffisante des services qu'il a rendus. Lorsque des problèmes surgissent, le comité de projet les reporte sur la « carte du risque » du projet, et la direction prend les mesures de suivi nécessaires, y compris l'application des pénalités contractuelles, le cas échéant.

Les entreprises devraient-elles aussi définir leurs propres normes déontologiques à l'endroit des tiers fournisseurs?
Après l'entrée en vigueur de la loi brésilienne anticorruption, la plupart des entreprises ont passé en revue leurs normes déontologiques et leur code de conduite; l'une des grandes nouveautés, c'est qu'elles y ont ajouté des procédures et des règles qui s'adressent aux tiers fournisseurs.

Par le passé, toutes les activités encadrant les règles de déontologie, comme la formation et les ateliers, étaient entreprises dans une perspective interne. Les normes s'appliquaient au personnel de l'entreprise, mais ne dépassaient pas les limites de celle-ci pour viser également les fournisseurs externes. Maintenant, la portée s'est élargie et les règles régissant les employés, les mesures de santé et de sécurité, les conditions de travail, l'obéissance aux lois, etc., englobent aussi les tiers fournisseurs. Les entreprises ont également étendu leurs programmes de formation et invitent leurs fournisseurs à leurs séminaires et ateliers où seront expliqués les règles et les processus de surveillance.

Par le passé, toutes les activités encadrant les règles de déontologie, comme la formation et les ateliers, étaient entreprises dans une perspective interne. Les normes s'appliquaient au personnel de l'entreprise, mais ne dépassaient pas les limites de celle-ci pour viser également les fournisseurs externes.

Personnes-ressources

Gestion des risques de contrats et de conformité

Timothy Scott
Associé, Service des risques d'entreprise
tiscott@deloitte.ca

Poonam Singh
Associée, Service des risques d'entreprise
posingh@deloitte.ca

Baskaran Rajamani
Associé, Service des risques d'entreprise
brajamani@deloitte.ca

Anne-Héloïse Bédard
Directrice principale, Service des risques d'entreprise
abedard@deloitte.ca

Gouvernance d'entreprise

Don Wilkinson
Leader, Centre canadien de gouvernance d'entreprise
dowilkinson@deloitte.ca

Chantal Rassart
Associée, Centre canadien de gouvernance d'entreprise
crassart@deloitte.ca

Si vous ne voulez pas rater les prochains numéros de *À l'ordre du jour du conseil*, rendez-vous sur la page du Centre de gestion des préférences de Deloitte (https://preferences.deloitte.ca/authentification) et sélectionnez tout simplement l'option Gouvernance d'entreprise.

Pour lire nos numéros précédents de la série *À l'ordre du jour du conseil* ou encore si vous souhaitez obtenir plus de renseignements sur ces sujets, visitez le Centre de gouvernance d'entreprise de Deloitte (www.gouvernance.deloitte.ca).

Des questions ou des commentaires? Communiquez avec nous à gouvernance@deloitte.ca.

www.gouvernance.deloitte.ca

Nous vous invitons à visiter notre Centre de gouvernance d'entreprise, où vous trouverez des ressources qui répondront aux besoins de votre conseil.

Remerciements

Le Centre mondial de gouvernance d'entreprise de Deloitte tient à remercier tous les professionnels qui nous ont aidés à rédiger, à mettre en forme et à réviser ce document, notamment ceux et celles dont le nom apparaît ci-dessous :

Coauteurs : Chantal Rassart (Canada) et Hugh Miller (Hugh Miller Communications).

Les réviseurs techniques de nos divers Centres de gouvernance d'entreprise : Michael Rossen (États-Unis), Timothy Scott (Canada), Kevin Tracey (États-Unis).