

LA ROULETTE EN MATIÈRE DE RÉGLEMENTATION ? DE MEILLEURES PROPOSITIONS POUR GÉRER LE RISQUE DE NON-CONFORMITÉ

Pendant des années, Apple Inc. a diffusé une série de publicités à la télévision expliquant aux consommateurs que pour toute situation, «il existe une application». Les entreprises, opérant dans l'environnement mondialisé actuel, pensent certainement la même chose de la réglementation.

Dans tous les secteurs et sur tous les territoires, pour chaque produit et pour chaque service, apparemment, «il existe une réglementation». Et la lourdeur de la réglementation ne cesse d'augmenter. Dans une étude mondiale conduite en 2015, l'International Federation of Accountants (IFAC) indiquait que 83 % des comptables avaient constaté un accroissement significatif des effets de la réglementation sur leur entreprise par rapport à 2010.

Malgré le développement de la réglementation et les risques encourus en cas de non-conformité, certaines sociétés ne prennent toujours pas suffisamment sérieusement la responsabilité qu'elles ont d'identifier et de gérer les risques liés à la conformité.

Une étude réalisée en 2014 par Deloitte et Com-

pliance Week a montré que 40 % des entreprises n'effectuaient pas d'évaluation des risques de conformité annuelle. Par ailleurs, une étude conduite en 2015

par l'IIA a déterminé que 38 % des Directeurs de l'audit n'utilisaient pas les obligations liées à la conformité ou aux réglementations comme ressource pour établir le plan d'audit.

Norman D. Marks, un ancien Directeur de l'audit et responsable des risques et de la conformité, auteur d'un blog pour le magazine *Internal Auditor* de l'IIA, a peut-être trouvé la raison de ce comportement : «Si les entreprises ne considèrent pas le risque de non-conformité comme un risque global pour leurs activités», déclare-t-il, «elles peuvent en sous-estimer les conséquences. La possibilité que cela puisse avoir des répercussions est pourtant bien réelle. Des activités peuvent être restreintes, une usine fermée. Tout cela peut avoir d'énormes

conséquences sur la réputation de l'entreprise, le moral des salariés peut en souffrir, et les ventes peuvent diminuer.» Comment les directeurs et les cadres dirigeants qui souhaitent mieux gérer les risques de



non-conformité doivent-ils procéder pour améliorer cette situation ?

Une bonne façon de commencer est de s'assurer que les rôles et les responsabilités en matière de gestion et de contrôle des risques sont bien définis et bien compris dans toute l'entreprise.

Les trois lignes de maîtrise

Le modèle des trois lignes de maîtrise prône la claire définition des responsabilités sur trois aspects des risques : la propriété des risques, le contrôle des risques et l'assurance des risques. Les fonctions qui possèdent et qui gèrent les risques constituent la première ligne. Les diverses fonctions de contrôle des risques et de conformité qui gèrent les risques constituent la deuxième ligne. Le rôle de l'audit interne (qui constitue la troisième ligne de maîtrise) fournit l'assurance aux parties prenantes (le conseil d'administration, le comité d'audit, les cadres) que les risques liés à la conformité peuvent être gérés à des niveaux acceptables. Définir le « niveau acceptable » (l'équilibre entre le coût potentiel du risque et la quantité de ressources nécessaire à sa limitation) fait bien sûr partie de la difficulté.

Le rôle de l'audit interne

De nombreux départements d'audit interne, indique Norman Marks, pratiquent deux types d'audits : le premier détermine si la conformité est bien respectée, et second détermine si des contrôles ont été mis en place pour pouvoir raisonnablement garantir le respect de la conformité. M. Marks estime que l'audit interne doit se concentrer sur la seconde catégorie et donner un avis sur la gestion des risques de non-conformité (et non un avis pour dire si la conformité est respectée ou pas). Pourquoi ? « C'est un objectif mouvant », précise-t-il. « Il est possible que l'entreprise soit conforme un jour, mais pas le lendemain. De plus, les auditeurs internes sont experts en procédures et en contrôles, pas nécessairement dans toutes les nuances et toutes les complexités de la loi et de la réglementation. »

La capacité de l'audit interne à jouer ce rôle peut être favorisée ou entravée par la structure dans laquelle il intervient. L'IIA recommande que l'audit interne dépende fonctionnellement du Conseil d'administration et administrativement du PDG pour aider à protéger l'indépendance de l'audit interne.

Travailler en partenariat pour mieux se prémunir des risques de non-conformité

Combinaison de la deuxième et la troisième lignes de maîtrise peut permettre d'offrir une assurance efficace contre le risque de non-conformité. Cette approche

consiste à coordonner les efforts de plusieurs fonctions internes d'assurance et de les associer, ce qui peut réduire la nature, la fréquence et la répétition des audits internes et limiter ainsi la lassitude que peuvent générer trop d'audits et de rapports auprès du Conseil d'administration ou de la direction générale. Pour réussir, l'audit interne et les fonctions internes chargées du contrôle (comme le département conformité), doivent travailler en partenariat pour assurer l'objectivité et la qualité de l'assurance délivrée.

Paul Sobel, Directeur de l'audit chez Georgia-Pacific LLC et ex-Président de l'IIA est favorable à ces partenariats, mais il reconnaît également qu'il peut être difficile d'obtenir une assurance véritablement objective, notamment lorsque la conformité dépend de l'audit interne ou vice versa, ou lorsque les deux domaines relèvent du même département. « Ce système de reporting doit faire l'objet de discussions avec la direction et le Conseil d'administration, et il faut envisager l'externalisation ou le co-sourçage de certaines activités de garantie de conformité pour arriver à l'objectivité », indique M. Sobel.



Les responsabilités du Conseil d'administration et du comité d'audit

Le Conseil d'administration et le comité d'audit jouent un rôle majeur dans la fonction des risques relatifs à la conformité. Que doivent-ils faire pour assumer leurs responsabilités de manière efficace ?

Même si les entreprises fonctionnent de façon sensiblement différente, les Conseils d'administration sont généralement chargés des responsabilités suivantes :

- Obtenir la garantie que la direction gère le risque de non-conformité. Demander à être alerté en cas de violation significative des lois ou des réglementations.
- Poser des questions à l'audit interne, à la direction et à la fonction conformité sur les capacités de l'entreprise. A-t-on les bonnes personnes et la bonne culture ? Si des employés identifient des dysfonctionnements, est-il garanti qu'ils seront rapportés et que des mesures seront prises ? Existe-t-il un niveau de garantie suffisant que l'entreprise respecte les normes et la réglementation en vigueur dans son secteur d'activité ?
- Obtenir une formation à la conformité. Apprendre quelles politiques de l'entreprise sont liées à la conformité et doivent faire l'objet de contrôles.
- Passer en revue les dysfonctionnements les plus importants, y compris en termes de performance, constatés au cours d'audits internes, par des demandes d'informations de parties prenantes externes ou encore dans l'historique des incidents. Demander à être informé de l'existence de problèmes répétés ou récurrents, et demander quels actions les dirigeants et/ou les comités d'audit ont mises en œuvre pour les résoudre.

Les responsabilités du comité d'audit en matière de risque de non-conformité peuvent aussi varier d'une entreprise à l'autre, mais elles doivent être clairement définies dans la charte du comité. De nombreux comités d'audit mettent en place des revues plus détaillées de la conformité. Dans certaines entreprises, c'est un comité de gouvernance qui peut s'en charger. Ces revues recouvrent des points trimestriels sur les changements de procédures, l'avancement des formations, des enquêtes, un état des infractions et autres problèmes relatifs à la conformité. Le Président du comité peut alors décider d'informer le Conseil d'administration, en fonction de la situation.

Le comité d'audit peut également demander au département d'audit interne d'auditer la deuxième ligne de maîtrise en se concentrant sur les risques stratégiques. Cela peut concerner par exemple des dysfonctionnements constatés ou encore des projets d'investissement. Le comité doit aussi identifier les lacunes dans

la connaissance et la mise en œuvre de la stratégie, en examinant les problèmes semblables ou récurrents sur plusieurs sites.

Par ailleurs, le comité d'audit et le Conseil d'administration doivent passer intégralement en revue le plan d'audit interne, le valider et vérifier qu'il est bien axé sur les risques opérationnels et de non-conformité appropriés, surtout lorsque les normes applicables au secteur d'activité ne reflètent pas forcément tous les risques que l'entreprise peut encourir. Par exemple, dans de nombreux secteurs, les entreprises s'appuient sur les normes internationales ISO (de l'International Organization for Standardization) qui, selon cette organisation, « indiquent les obligations, les spécifications, les directives ou les caractéristiques qui peuvent être utilisées de manière systématique pour garantir l'adéquation des matériaux, des produits, des procédures et des services. » Peter Montagna, Directeur des évaluations et de l'audit concernant la santé, la sécurité et l'environnement (SSE) chez Henkel, déclare : « Le comité d'audit et/ou l'équipe de direction qui commandite des audits doit clairement dire que l'identification des écarts par rapport aux normes est secondaire par rapport à l'identification des risques. Ainsi, les opérationnels peuvent prendre des mesures appropriées et la direction peut avoir l'assurance que les risques pour la santé, la sécurité et l'environnement sont bien contrôlés. »

L'accroissement des responsabilités du Conseil d'administration et du comité d'audit sont des indicateurs clairs que le risque de non-conformité prend une importance prééminente dans le portefeuille des risques des entreprises. L'audit interne est également concerné. Mais Norman Marks met aussi en garde par rapport au fait d'accorder une importance exclusive aux risques de non-conformité : « Les comités d'audit et les cadres doivent comprendre que le risque de non-conformité n'en est qu'un parmi les nombreux types de risques sur lesquels l'audit interne doit travailler. L'audit interne doit consacrer la majeure partie de ses ressources aux risques susceptibles de compromettre la réussite de l'entreprise et la réalisation de ses objectifs. Les risques de non-conformité ne sont pas tous suffisamment importants pour figurer dans le plan d'audit. »

Sondage rapide

Indiquez, en attribuant une note, dans quelle mesure vous êtes d'accord avec la déclaration suivante : J'ai confiance dans le fait que les risques de non-conformité sont suffisamment garantis dans mon entreprise.

Allez sur www.theiia.org/tone pour répondre à la question et voir comment d'autres personnes y répondent.

L'IIA

L'Institute of Internal Auditors Inc. (IIA) est une association professionnelle internationale qui compte plus de 185 000 membres dans plus de 170 pays et territoires. L'IIA intervient en tant que principal défenseur de l'activité d'audit interne qui en fixe également les normes, et en tant que principale structure de recherche et de formation dans ce domaine.

www.globaliia.org

Abonnements gratuits

Consultez www.theiia.org/tone ou appelez le +1-407-937-1111 pour commander votre abonnement gratuit.

Avis des lecteurs

Envoyez vos questions/commentaires à tone@theiia.org.

Conseil consultatif examinant le contenu

Ayant plusieurs dizaines d'années d'expérience de la Direction d'entreprise et des Conseils d'administration, les personnes suivantes, qui sont des professionnels reconnus, donnent des orientations sur le contenu de cette publication :

Martin M. Coyne II
Kenton J. Sicchitano

Michele J. Hooper

TONE [®]
— at the — TOP

247 Maitland Avenue
Altamonte Springs, Florida 32701-4201

ORGANISATION À BUT
NON LUCRATIF
PORT PAYÉ ÉTATS-UNIS
THE INSTITUTE OF
INTERNAL AUDITORS

Résultats du sondage rapide :

Quel modèle répond-il le mieux aux intérêts de votre entreprise ?

10%

L'association des fonctions de PDG et de Président du Conseil d'administration

80%

La distinction des fonctions de PDG et de Président du Conseil d'administration

10%

L'association des fonctions de PDG et de Président du Conseil d'administration avec la désignation d'un Directeur principal indépendant

Basé sur 177 réponses. Source : Étude d'août 2016 *Tone at the Top* The IIA.