L'ANALYSE

La compliance, la fonction pivot d'une entreprise

La fonction « conformité » ou de compliance est devenue en l'espace de quelques années un des piliers de la gouvernance d'une société.

La crise financière de 2008 a provoqué une rupture dans la façon d'appréhender les normes et dans la manière de diriger l'entreprise. La fonction « conformité » au sein de l'entreprise n'a depuis cessé de se transformer, renouvelée constamment par les réglementations. Pour la plupart des dirigeants, le respect de cet ensemble de normes s'est mué en un objectif supérieur dans leur gouvernance.

Qu'il s'agisse de la loi Sapin 2 du 9 décembre 2016 sur les dispositifs de lutte contre la corruption, de l'implémentation du règlement général sur la protection des données (RGPD) du 27 avril 2016, du devoir de vigilance des sociétés-mères et des entreprises donneuses d'ordre (loi du 27 mars 2017) ou encore de la prévention du risque cyber (décret d'application du 25 mai 2018 de la directive NIS), ces réglementations ont toute un impact opérationnel lourd et immédiat sur les entreprises et leurs dirigeants. En outre, la responsabilité personnelle des dirigeants est régulièrement renforcée à l'occasion de la mise en œuvre de ces nouvelles dispositions.

Il n'existe toutefois pas encore de principe général instaurant une direction de la compliance ou de l'éthique des affaires dans les entreprises. Néanmoins des exceptions existent dans le domaine de la finance où les banques et les assureurs ont l'obligation de mettre en place cette fonction, qui est d'ailleurs qualifiée de fonction clé par la directive Solvabilité 2 pour l'assurance. D'autre part des exceptions par domaine se créent et les entreprises françaises, depuis la loi Sapin 2 du 9 décembre 2016, ont l'obligation de mettre en place un dispositif de conformité pour lutter contre la corruption, qui doit donc tout naturellement être confiée à une direction dédiée. L'Agence française anticorruption (AFA) a publié un guide pratique en ce sens en janvier 2019 intitulé : La fonction conformité anticorruption dans l'entreprise.

© PRÉNOM NOM / AGENCE

● **CÉDRIC DUCHATELLE,** DIRECTEUR GROUPE CONFORMITÉ & ÉTHIQUE DES AFFAIRES AU SEIN D'AG2R LA MONDIALE.

Prévention des risques et protection de l'entreprise

Dans ce contexte, la définition de la compliance que je propose est la suivante : « *la compliance est d'abord une culture qui vise à intégrer dans le processus de gouvernance – c'est-à-dire l'organe de décision d'une entreprise – une connaissance et une prise en compte adaptée des risques de non-conformité. C'est ensuite une méthode de vérification de la conformité déployée afin de protéger, de conseiller et d'anticiper la survenance d'un risque de réputation, induisant des pertes significatives pour l'entreprise.* »

Cette définition est issue du croisement d'une pratique professionnelle, d'une activité d'enseignement de la compliance et de la confrontation d'idées au sein d'associations professionnelles. Elle permet de comprendre que la compliance, contrairement à ce que pourrait laisser entendre le mot de conformité, n'est pas réductible à une technique ou à une nouvelle matière juridique. Nous sommes très loin de la simple exécution de *process* qui transformeraient les collaborateurs de l'entreprise en opérateurs. Au contraire, c'est au travers d'un réseau de terrain que la direction conformité sera en mesure de comprendre ce qui est réellement mis en œuvre dans l'entreprise et de conseiller la direction générale sur les éventuelles mesures à mettre en œuvre, ainsi que les priorités à dégager sous l'angle des exigences réglementaires.

Véritable garde du corps de l'entreprise et de ses dirigeants, une direction conformité permettra de prévenir les risques et de protéger l'entreprise comme les responsables qui la dirigent. La direction « compliance » doit donc connaître les principaux risques de non-conformité réellement présents dans l'entreprise. Ces risques peuvent être le fait d'anciennes réglementations mal ou pas appliquées dans l'entreprise, comme celle de nouvelles non identifiées ou insuffisamment prises en compte.

© PRÉNOM NOM / AGENCE

Avec la multiplication des risques encourus par les entreprises… mettre en place une direction conformité devient une nécessité.

Les typologies de « non-conformité »

Une direction compliance doit être en lien avec l'ensemble des directions opérationnelles afin de les accompagner dans la mise en œuvre des projets réglementaires et de vérifier que les solutions déployées sur le terrain ne présentent pas de risques majeurs pour l'entreprise.

La connaissance du terrain et de la réalité opérationnelle constitue la matière première d'une direction compliance. C'est à partir de celle-ci que le travail de filtrage et de tri doit intervenir afin de dégager entre tous les éléments, ceux qui présentent des risques suffisamment sérieux pour retenir l'attention.

Classer les risques

Plusieurs situations sont à distinguer. D'une part, les non-conformités minimes qui peuvent faire l'objet de recommandations de mise en œuvre mais ne sont pas prioritaires. Elles devront être suivies mais sans exercer de pression particulière sur les métiers. C'est l'opportunité d'une réforme plus large qui permettra de les solutionner. Aucune communication spécifique n'apparaît nécessaire sur ces non-conformités mineures.

D'autre part, les non-conformités majeures c'est-à-dire celles qui, sans plan de remédiation, peuvent exposer l'entreprise. Une gradation entre ces non-conformités peut être envisagée pour les distinguer si elles sont trop nombreuses en intégrant le risque attaché à l'impact et la probabilité de survenance. Mais ce qui est surtout intéressant d'identifier c'est l'existence ou non d'un plan d'action de remédiation. Ce dernier doit être sérieux pour être recevable. Il doit comporter un pilote, une planification, des livrables… L'action d'une direction conformité est à cet égard importante pour accompagner les fonctions opérationnelles en charge du plan d'action pour s'assurer que ce dernier répond bien aux exigences réglementaires. La formulation des recommandations par la direction conformité sera à cet égard structurante. Plus la recommandation sera précise et opérationnelle, plus les fonctions métiers seront en capacité de la mettre en œuvre.

À retenir

La compliance est une connaissance et une prise en compte des risques de non-conformité dans le processus de gouvernance d'une entreprise.

À noter

Propre au secteur de la banque et de l'assurance, il n'existe pas encore d'obligation d'instaurer une direction de la compliance ou de l'éthique des affaires au sein de l'entreprise.

Conseiller la direction générale

Une direction conformité doit donc, à titre principal, être en mesure de conseiller la direction générale sur les orientations notamment budgétaires à mettre en œuvre afin de couvrir les principales obligations de mise en conformité et les risques avérés les plus importants. Dans l'idéal, il faudrait que l'entreprise puisse être totalement conforme à l'ensemble des points réglementaires. En pratique, l'enjeu est d'abord de conseiller la direction générale sur les priorités à retenir et sur le calendrier acceptable de mise en œuvre de celles-ci. Ce dernier point ne doit pas être négligé car il est souvent le reflet des ressources allouées par une entreprise à ces sujets de mise en conformité.

En conclusion, une direction conformité ne sera pas décisionnaire sur les arbitrages et les choix de faire ou ne pas faire. La décision relève en premier ressort des directions métiers responsables opérationnels et en dernier ressort de la direction générale sous le contrôle des conseils d'administration. Il est enfin important que la direction générale soit le sponsor de la direction compliance afin que cette dernière puisse accéder en toute indépendance à toutes les informations nécessaires à l'exercice de ses missions auprès d'elle. ●