L'audit de la culture d'éthique et de *compliance* de l'entreprise

George Fife, Associé, Fraud Investigation & Dispute Services, Ernst and Young et Associés

Jean-Yves Trochon, Senior Advisor, Fraud Investigation & Dispute Services, Ernst and Young et Associés

Ethique et compliance : deux notions antinomiques ? Les auteurs démontrent, au contraire, que ces valeurs sont intimement liées et ils proposent des pistes judicieuses et concrètes pour évaluer et promouvoir le niveau de maturité de la culture éthique de l'entreprise dans le plan d'audit.

L'émergence de la notion de *compliance* et les obligations pour les entreprises de mettre en place un dispositif robuste de prévention, de détection et de remédiation des risques de non-conformité à la loi sapin II conduisent à se poser la question de l'audit de la culture, des valeurs et de l'éthique de l'entreprise.

Cette question est d'autant plus essentielle dans le contexte actuel des affaires marqué par une pression accrue sur le développement de l'activité, notamment à l'international, dans des pays où les risques de corruption sont élevés. Les conséquences des affaires de corruption, de fraude ou autre peuvent avoir un impact considérable sur l'entreprise : sanctions financières, mais aussi risques d'atteinte à leur réputation, risques d'exclusion des marchés publics, ou encore risques de mise en cause de leur responsabilité pénale (dirigeants et personnes morales). Pour cette raison, le socle d'un programme efficace de gestion des risques de *compliance* repose sur la création et le développement, avant toute chose, d'une culture de la *compliance*. Celle-ci doit être intrinsèque à l'organisation.

Outre les risques de corruption, bien d'autres cas de violations des réglementations peuvent avoir des effets tout aussi dévastateurs pour l'entreprise. Pratiques dites de cartels, conflits d'intérêts abusifs, non-respect des règles en matière de données personnelles, contrôle des exportations, sanctions et embargos, etc. Tous doivent faire l'objet (au même titre que la corruption au sens large) de mesures de vigilance particulières.

Les principes d'action et les codes de conduite traditionnels sont progressivement dépassés et remplacés par des programmes d'éthique et de *compliance*. Les entreprises affirmaient des valeurs, elles doivent désormais développer des politiques, des procédures et des guides d'application à destination de leurs collaborateurs. Mais surtout, elles doivent veiller à ce que ces règles internes soient strictement appliquées afin de limiter leurs risques d'exposition à des sanctions financières, pénales ou médiatiques potentiellement « mortelles ».

Ces efforts de structuration autour de tels dispositifs resteront toutefois vains si l'entreprise ne dispose pas d'une véritable culture éthique. C'est à travers cette notion que l'on peut mesurer l'efficacité des mesures mises en place pour permettre une croissance pérenne du modèle économique grâce à une bonne maitrise des risques d'éthique et de non-conformité.

Nous utiliserons ici le terme de « culture éthique », de préférence à celui d'intégrité couramment utilisé aux États-Unis, même si les deux termes recouvrent les mêmes notions et enjeux. Deux aspects méritent une attention particulière :

- Comment appréhender la culture d'éthique et de *compliance* de l'entreprise ?
- Comment intégrer la culture d'éthique et de *compliance* dans le plan d'audit ?

Comment appréhender la culture d'éthique et de *compliance* de l'entreprise ?

La culture de l'entreprise *lato sensu* est un sujet bien connu. En revanche, la notion de culture éthique – au sens « éthique et *compliance* » – est relativement récente lorsque l'on cherche à en dresser des contours précis.

En effet, la culture doit susciter une adhésion réelle de chaque collaborateur et dirigeant de l'organisation à un corpus de valeurs, et surtout de normes internes érigées en cohérence avec ces valeurs.

Or, dans une vision négative, ces normes sont par définition contraignantes ; elles apparaissent même, à certains égards, comme des freins au développement de l'entreprise, voire des obligations bureaucratiques inutiles et coûteuses. Aux yeux de certains, la *compliance* serait presque antinomique de la notion d'éthique, qui repose sur une logique de confiance en la capacité des collaborateurs de conformer naturellement leurs comportements aux valeurs de l'entreprise (responsabilité, bienveillance, courage, esprit d'équipe, etc.).

Pourtant, il est aujourd'hui incontestable qu'un programme de compliance structuré, déployé et contrôlé, fondé sur une organisation appropriée, est un élément-clé de bonne gouvernance et de gestion des risques. La dichotomie éthique et compliance apparait artificielle à cet égard, car si l'éthique inspire la *compliance*, une éthique sans mesures rigoureuses de compliance aidant l'entreprise à respecter ses engagements est inenvisageable.

L'objectif de l'organisation est donc bien de développer une culture d'éthique et de *compliance*. On pourrait la définir comme l'ensemble des systèmes de management mis en œuvre pour fournir une assurance raisonnable au Conseil d'administration que les comportements des collaborateurs, dirigeants et principales parties prenantes s'inscrivent dans le respect des lois, des réglementations, mais aussi des valeurs éthiques de l'entreprise. Ces dernières sont par construction fondées sur le respect des lois et réglementations applicables à l'entreprise, mais elles vont au-delà car :

- elles fournissent une grille d'interprétation des normes de *compliance* au regard de l'environnement et du business model de l'entreprise ;
- elles dépassent l'objectif de conformité aux lois et règlementations applicables au travers d'engagements volontaires.

Par exemple, les décisions d'implantation internationale ou d'exportation dans certains pays devront être validées, non seulement au regard de la conformité avec les lois et réglementations, mais aussi à la lumière d'autres critères dits éthiques : promotion, environnement, droits de l'Homme, gouvernance des États, capacité à intégrer de nouvelles équipes habituées à des pratiques éloignées de la culture du groupe, impact sur la réputation, etc. De même, les activités de R&D, le lancement de nouveaux produits ou la réponse à certains appels d'offres doivent intégrer les considérations éthiques (attentes des consommateurs, des populations locales, de l'opinion publique et des médias, etc.). À titre d'illustration, la décision de participer ou non à la construction du mur entre les États-Unis et le Mexique constitue actuellement un « dilemme éthique ».

> « *Les principes d'action et les codes de conduite traditionnels sont progressivement dépassés et remplacés par des programmes d'éthique et de* compliance »

Dès lors, chaque entreprise peut s'appuyer sur un référentiel de culture éthique adapté à son environnement et son *business model*. Un tel référentiel ne se limitera pas aux cartographies de risques, aux plans de vigilance, aux dispositifs de contrôles internes et aux programmes de *compliance* ; il devra aussi prendre en compte une gouvernance adaptée, un dispositif d'alerte et d'investigation rigoureux, ou encore un mécanisme de prise en considération des attentes légitimes des parties prenantes de l'entreprise. Enfin et surtout, il devra faire l'objet d'un plan d'audit et de *monitoring* fondé sur des indicateurs quantitatifs et qualitatifs.

Comment intégrer la culture éthique dans le plan d'audit ?

Chaque entreprise doit définir la manière idoine de procéder à l'audit de sa culture éthique en poursuivant un triple objectif :

- mesurer le niveau de maturité de la culture éthique de l'entreprise à travers l'efficacité des dispositifs de *compliance* et de contrôle interne, mais aussi de la gouvernance de l'entreprise ;
- recommander les mesures appropriées pour développer cette culture et remédier aux points de faiblesse détectées lors des audits ;
- contribuer à l'amélioration continue du dispositif de « *monitoring* ». La culture éthique n'est pas l'apanage des seules fonctions d'audit, de contrôle interne ou de *compliance* ; elle relève aussi de la responsabilité des opérationnels confrontés aux problématiques de terrain.

Ainsi, le plan d'audit devrait-il prendre en considération les éléments suivants :

- « *Tone at the top* » : le haut management communique-il clairement sur l'importance qu'il attache au respect sans compromis des dispositifs de contrôle interne et de compliance, ainsi qu'aux principes éthiques affichés par l'entreprise ?
- **Gouvernance :** les organes de gouvernance soutiennent-ils sans ambiguïté le haut management dans cette démarche ? Des règles de gouvernance appropriées ont-elles été établies pour examiner les principales décisions stratégiques à l'aune de ces critères ?
- **Dispositifs d'éthique, de conformité et de contrôle interne :** les dispositifs en place permettent-ils de contrôler efficacement les principaux risques d'éthique et de *compliance* de l'entreprise (corruption, trafic d'influence, conflits d'intérêts, données personnelles, plan de vigilance des tierces-parties, LCB/FT, sanctions, embargos, *export control*, droits de l'Homme, concurrence, règlementations spécifiques au secteur, etc.) ?
- **Ces dispositifs sont-ils effectivement déployés et « managés » ?** Le ou les *compliance officers* disposent-ils de l'autonomie, des ressources nécessaires et de la vision 360° pour leur mission ? Ont-ils un

accès effectif au plus haut niveau de la hiérarchie ?

- **Formation des collaborateurs :** les collaborateurs sont-ils régulièrement formés au respect de ces dispositifs ? Existe-t-il des mesures d'évaluation de ces programmes de formation ? Les collaborateurs peuvent-ils consulter les *compliance officers* pour obtenir une *guidance* claire et opérationnelle en cas de dilemmes éthiques ? Ne risquent-ils pas d'être pénalisés quant à la réalisation de leurs objectifs ?
- **Ressources humaines :** les questions d'éthique, y compris l'éthique dite « employeur », sont-elles suffisamment prises en compte dans les processus RH (notamment dans la définition des objectifs ou vis-à-vis des comportements contraires au bien-être au travail de certains collaborateurs) ? Le « management par l'exemple » est-il respecté ? Comment le mesure-t-on ?
- **Communication :** existe-t-il une communication effective sur l'importance du respect attaché par l'entreprise aux dispositifs d'éthique et de *compliance*, y compris celui de gestion des alertes et de protection des lanceurs d'alertes (par exemple sous forme de sondages anonymes des salariés) ?
- **Gestion des alertes :** le dispositif de gestion des alertes et des investigations est-il « mature » ? La procédure existante protège-t-elle les lanceurs d'alerte ? Les alertes font-elles systématiquement l'objet d'une investigation ? Ces investigations sont-elles effectuées de manière confidentielle et indépendante ?
- **Transparence :** quel est le degré de transparence de l'entreprise en matière d'éthique en interne, mais aussi vis-à-vis des parties prenantes ? La communication extra-financière aborde-t-elle ces questions de manière ouverte ?

> ***« La culture doit susciter une adhésion réelle de chaque collaborateur et dirigeant de l'organisation à un corpus de valeurs »***

* *
*

Au vu des exigences accrues des régulateurs et des parties prenantes (notamment actionnaires et salariés) comme des niveaux de sanctions sans cesse croissants, l'audit de la culture d'éthique et de *compliance* de l'entreprise revêt un enjeu de plus en plus important.

Il suppose néanmoins que l'entreprise ait d'abord mis en place un dispositif de *compliance* cohérent avec son référentiel de contrôle interne, sur la base des bonnes pratiques attendues en la matière. À cet égard, la loi Sapin II devrait aider les entreprises à construire ou développer ces dispositifs, à travers notamment l'exigence de mise en place de codes de conduite, de cartographie des risques, de recueils des alertes ou encore de mesures de *monitoring*. Rappelons toutefois que la culture d'éthique et de *compliance* ne se résume pas à la seule loi Sapin II qui ne concerne « que » la corruption et le trafic d'influence. ■

Nouveau COSO ERM

Au moment où nous lançons l'impression du présent numéro, l'IIA vient d'adresser à l'IFACI la **nouvelle version du « COSO Entreprise Risk Management »** publiée avec un nouveau sous-titre très signifiant « ***Integrating with Strategy and Performance*** » illustré par le schéma ci-dessous.

L'IFACI ne manquera pas de revenir sur les composantes et les principes de cette démarche renouvelée.