



Points d'attention 2017 pour les conseils d'administration

Audit Committee Institute

En 2017, la performance des entreprises reposera encore sur certains éléments essentiels, tels que la gestion des principaux risques, l'innovation et la captation des nouvelles opportunités, et l'exécution diligente de la stratégie. Cependant, le contexte connaît une évolution rapide, et peut-être même profonde. Les sociétés et leurs conseils d'administration sont incités à repenser le développement et l'exécution de leur stratégie, ainsi que ce que signifie être leader, en raison des avancées technologiques, de la remise en cause des « business models », des attentes toujours plus élevées des investisseurs et autres parties prenantes, des changements politiques et d'une volatilité globale généralisée. Sur la base de notre enquête récente et de nos échanges avec les dirigeants d'entreprises au cours de l'année écoulée, nous avons dressé la liste des sept enjeux clés que les conseils d'administration doivent garder à l'esprit pour guider leurs entreprises en 2017.

1

Reconnaître qu'il est plus important - et plus difficile - que jamais de corrélérer et d'aligner la stratégie et les risques.

Tant de choses peuvent changer en quelques mois. Le vote relatif au Brexit et l'élection de Donald Trump aux États-Unis, qui ont pris au dépourvu la plupart des observateurs - et bouleversé de nombreuses stratégies d'entreprises - auront des conséquences significatives sur les marchés internationaux et le contexte géopolitique dans son ensemble. Le fait que ces changements radicaux aient été largement imprévus en dépit des analyses complètes réalisées en amont constitue pour les entreprises un rappel brutal qu'il est possible de passer à côté des signaux du marché (que cela soit lié à la tendance à se satisfaire de la situation actuelle sans volonté d'évoluer, à celle de favoriser ce que l'on connaît, ou encore à une « complaisance de confort ») et que les règles du jeu peuvent être fondamentalement modifiées du jour au lendemain. Si le contexte géopolitique est voué à s'éclaircir, l'environnement concurrentiel restera dynamique et opaque, exigeant une grande réactivité. En raison notamment des avancées technologiques, des innovations incessantes, de la remise en cause des « business models », de l'arrivée sur le marché du travail de la nouvelle génération du Millénaire et d'autres changements démographiques, ainsi que de l'évolution

des demandes des clients et des attentes des salariés, l'agilité et la capacité de retournement des entreprises seront essentielles. Il est nécessaire de tenir compte des transformations constantes, de la gestion des risques liés aux talents et des opportunités qu'offrent les « nouvelles » technologies. La direction a-t-elle mis en place un processus efficace permettant de contrôler les changements de son environnement et d'apprécier la validité des hypothèses sur lesquelles reposent sa stratégie et sa politique en matière de risques ? Ce processus permet-il d'alerter en amont sur les éventuels ajustements nécessaires ? Le conseil dispose-t-il des talents et d'une vision prospective adéquats pour faire les liens requis entre les facteurs exogènes et la stratégie et le profil de risque de l'entreprise ? Le débat sur la stratégie doit être un processus continu tout au long de l'année (et pas uniquement l'objet d'une « décision » ponctuelle une fois l'an) intégrant à la fois une prise de risque intelligente et un processus solide d'établissement de scénarios tenant compte de multiples hypothèses. La stratégie et le risque doivent donc être intrinsèquement liés et se trouver au cœur de chaque discussion du conseil.

2

Développer et exécuter la stratégie en fonction de son incidence globale.

Comme indiqué précédemment, l'environnement dans lequel évoluent les entreprises change rapidement, au fur et à mesure que des forces politiques, sociales et réglementaires redessinent le paysage concurrentiel. Le rôle de l'entreprise au sein de la société passe progressivement au cœur des débats, tandis que les attentes des investisseurs, clients, employés et autres parties prenantes l'incitent à mieux comprendre

l'incidence globale de sa stratégie et de ses activités. Le développement et la mise en œuvre de la stratégie nécessitent l'adoption d'une approche globale incluant l'ensemble des risques et opportunités (notamment financiers, réglementaires, ou liés à la réputation, aux ressources et aux talents) qui affectent l'entreprise et ses nombreuses parties prenantes sur le long terme.

3

Se pencher sur la composition du conseil d'administration : les talents dont il dispose sont-ils cohérents avec la stratégie et les besoins futurs de l'entité ?

Compte tenu des exigences liées au contexte économique et à l'environnement des risques (ainsi qu'à l'intensification de la surveillance exercée par les investisseurs, les régulateurs et les médias), l'alignement des talents composant le conseil avec la stratégie de l'entité doit être une priorité (à court terme comme à long terme, puisque la stratégie évolue). Il n'est pas surprenant que 43 % des répondants à notre enquête récente intitulée « Qu'est-ce qu'un conseil d'administration efficace ? » aient cité la « résistance aux changements » et « l'inertie du statut quo » comme étant les principaux obstacles à la constitution d'un conseil performant. Il est bon de tenir compte des recommandations du rapport de la commission Blue Ribbon du NACD sur la composition du conseil en tant qu'actif stratégique (NACD Report on Building the Strategic Asset Board) et du rapport de la

WCD et de KPMG sur un conseil visionnaire (Seeing Far and Seeing Wide: Moving Toward a Visionary Board).

Comme l'indiquent ces rapports, les administrateurs doivent concentrer résolument leurs efforts sur la composition/ la diversité du conseil et les plans de succession, des évaluations efficaces, la limitation des mandats, le recrutement et l'intégration des nouveaux administrateurs, la présidence du conseil, la communication avec les parties prenantes, ainsi que la formation continue des administrateurs, et ce en prenant en compte les spécificités de l'entité et de son secteur d'activité. Ainsi, les remaniements périodiques du conseil doivent être remplacés par une approche d'amélioration continue et d'organisation active de plans de succession.

4

Accorder une attention particulière aux risques éventuels liés aux valeurs affichées par le Management, à la culture de l'entreprise et aux avantages incitatifs qu'elle accorde.

S'il est essentiel de mettre en œuvre un processus de gestion des risques efficace pour prévenir et limiter la survenance d'événements à risques, cela ne suffit pas. Comme nous l'avons vu ces dernières années, nombre de crises ayant le plus fortement affecté les entreprises (en termes financiers, juridiques et de réputation) ont été causées par une 'fracture' dans les valeurs, la culture et la politique en matière d'avantages incitatifs. Par conséquent, le conseil doit accorder une attention

particulière à ces risques fondamentaux qui sont les plus susceptibles d'affecter l'entité. Dans le contexte économique actuel, le conseil doit, aujourd'hui plus que jamais, être sensible au ton donné par la direction (et à l'exemple qu'elle montre) et au renforcement de la culture propre à l'entité : autrement dit, ce que fait l'entreprise, comment elle le fait, sa culture de conformité aux lois et règlements, son engagement vis-à-vis de la gestion de ses principaux risques.

5

Réévaluer le dispositif de l'entreprise en matière de prévention et de plan de gestion des crises.

La prévention et les plans de gestion des crises revêtent une importance et un caractère d'urgence accrus pour les conseils et les équipes dirigeantes, alors que la liste des crises auxquelles sont confrontées les entreprises s'est sensiblement allongée ces dernières années. La prévention des crises est indissociable d'une bonne gestion des risques, notamment l'identification et l'anticipation des risques, ainsi que la mise en place d'un système de contrôle visant à éviter les événements à risques et à atténuer leurs incidences s'ils se réalisent. Aujourd'hui, les conseils se concentrent davantage sur les grands risques opérationnels pour l'ensemble de leur organisation à l'échelle mondiale, tels que les risques au niveau de la chaîne d'approvisionnement et ceux liés à la sous-traitance, ainsi qu'aux technologies de l'information et à la sécurité des données, etc. Mais le conseil a-t-il une compréhension précise des risques opérationnels majeurs de l'entité ? Qu'est-ce qui a changé dans

l'environnement opérationnel de celle-ci ? L'entreprise a-t-elle subi des défaillances en matière de contrôles ? La direction est-elle sensible aux signes avant-coureurs d'incidents de sécurité, de qualité des produits et de conformité ? Bien entendu, même les entreprises les mieux préparées ne sont pas à l'abri d'une crise, mais celles qui savent réagir rapidement et efficacement, notamment par de solides plans de communication, ont tendance à mieux les affronter. Il faut déterminer si les plans de crise de l'entité sont cohérents avec son profil de risque, apprécier la fréquence avec laquelle les plans sont remaniés, et dans quelle mesure la direction – et le conseil – réalisent des exercices de simulation de crise. Des processus permettant d'informer régulièrement le conseil des divers événements survenus ainsi que des mesures prises en réaction par l'entreprise ont-ils été mis en place ?

6

Ré-apprécier le programme relationnel de l'entreprise avec ses actionnaires

L'implication auprès des actionnaires devient l'une des grandes priorités des entreprises, car les investisseurs institutionnels tiennent les conseils pour responsables des performances des sociétés et exigent davantage de transparence, ainsi qu'une relation directe avec des administrateurs indépendants. Ils s'attendent à échanger avec les sociétés de portefeuille, notamment lorsqu'ils se préoccupent des questions de gouvernance ou lorsque cela est nécessaire à une prise de décision éclairée en matière de vote de résolutions. Dans certains cas, les investisseurs exigent un dialogue avec les administrateurs indépendants. En conséquence, le conseil doit obtenir des informations régulières de

la part de la direction concernant ses pratiques en matière de relations avec les actionnaires : l'entreprise connaît-elle et s'implique-t-elle auprès de ses principaux actionnaires ? Comprend-elle leurs priorités ? L'équipe en charge de la relation avec les investisseurs est-elle composée des bonnes personnes ? Que pense le conseil des réunions avec les investisseurs ? Parmi les administrateurs indépendants, lesquels devraient être impliqués ? Stratégie, rémunération des dirigeants, efficacité et performance des dirigeants, initiatives environnementales et durables, composition et efficacité du conseil sont très probablement des thématiques figurant sur le radar des investisseurs.

7

Approfondir et élargir les discussions du conseil relatives aux risques liés à la cybercriminalité et à la sécurité.

Bien que la cybersécurité figure déjà au cœur des débats, les contours du périmètre des risques liés à la cybercriminalité restent flous et obscurs et ce, même s'il s'exprime des attentes accrues pour une supervision renforcée. Le paysage cybernétique évoluant, la supervision du conseil et la nature de ses échanges sur le sujet doivent également évoluer. Il ne s'agit plus tant de prévention que de détection et d'endiguement de ces risques. Les débats portent de plus en plus sur les « offres et solutions élargies » de l'entreprise qui peuvent constituer autant de points d'entrée supplémentaires pour les pirates informatiques. L'Internet des objets et les informations numériques qui entourent les gens, les organisations, les processus et les produits (« code halos ») exigent des échanges plus approfondis – voire même tout à fait différents. Le conseil a pour rôle d'accroître la sensibilité de l'ensemble de l'entreprise – y compris ses dirigeants – aux risques liés à la cybercriminalité, et d'aider à s'assurer qu'ils sont gérés comme des risques globaux susceptibles d'affecter l'activité ou l'entreprise toutes entières, et pas uniquement ses systèmes informatiques. Est-ce que les discussions relatives aux fusions-acquisitions, au développement

des nouveaux produits, à l'expansion géographique, aux relations avec les fournisseurs, les clients, les partenaires et sous-traitants, les conseillers et autres parties prenantes, tiennent compte des risques liés à la cybercriminalité ? En veillant au développement d'un état d'esprit sécuritaire, à la mise en œuvre d'une formation adaptée et à la préparation anticipatoire de la résolution des incidents, le conseil aide à promouvoir la sensibilisation et la responsabilisation de l'ensemble de l'organisation en matière de cybersécurité. Le conseil prévoit-il suffisamment de temps, dans son agenda, pour traiter, de manière régulière, des risques liés à la cybersécurité ? Est-il nécessaire qu'il crée un comité spécialisé distinct dédié à la cybersécurité ? Quels sont les principaux points de vulnérabilité de l'entreprise dans ce domaine et comment protège-t-elle ses données les plus importantes ? Se compare-t-elle aux autres entités du même secteur ? A-t-elle élaboré une fiche d'évaluation en matière de cybersécurité et un plan d'actions robuste en cas d'incident cybernétique ? Les administrateurs sont-ils conscients que chacun de leurs e-mails est susceptible d'être rendu public à tout moment ?

Voir aussi les « Points d'attention 2017 pour les comités d'audit » sur www.audit-committee-institute.fr

Contacts

Patrick-Hubert Petit

Associé
Président de l'ACI France
Tél : +33 (0)1 55 68 70 80
E-mail : ppetit@kpmg.fr

Site : audit-committee-institute.fr
E-mail : fr-auditcommittee@kpmg.com

Jean-Marc Discours

Associé
Responsable de l'ACI France
Tél : +33 (0)1 55 68 68 83
E-mail : jdiscours@kpmg.fr

Stella Vitchérian

Associée
Tél : +33 (0)1 55 68 68 30
E-mail : svitchenian@kpmg.fr