

Les Echos du Cercle de la Gouvernance

Session de janvier 2026

KPMG. Make the Difference.

Facilité par le Board Leadership Center, le Cercle de la Gouvernance de KPMG offre aux administrateurs un espace d'échanges entre pairs sur les enjeux clés de la gouvernance, en confrontant expériences, points de vue et témoignages. La publication « **Les Echos du Cercle de la Gouvernance** » rapporte la synthèse de ces échanges.

Thématiques clés abordées

Accédez à la rubrique souhaitée en un clic 

Cyber et Gouvernance

ESG et Gouvernance

AVANT-PROPOS

À l'heure où les organisations font face à des exigences réglementaires accrues, à des ruptures technologiques rapides et à des attentes renforcées de leurs parties prenantes, le rôle des Conseils continue d'évoluer en profondeur.

Les échanges du Cercle de la Gouvernance illustrent cette transformation. Parmi les sujets désormais incontournables, l'IA s'impose à l'agenda des Conseils. Portée par les usages métiers, elle transforme les modèles opérationnels, les compétences attendues et l'équilibre des responsabilités. Elle ouvre des perspectives de création de valeur, tout en soulevant des questions d'éthique, de sécurité et de souveraineté technologique.

Sur le terrain de la durabilité, la mise en œuvre de la CSRD mobilise encore fortement les entreprises. Si la double matérialité devait aider à hiérarchiser les enjeux stratégiques, sa traduction opérationnelle soulève de nombreuses difficultés : multiplication des IROs, arbitrages méthodologiques, contraintes de calendrier et montée en compétence des comités spécialisés. Pour les administrateurs, l'enjeu est désormais d'éviter que l'effort consacré aux aspects de reporting ne prenne le pas sur la réflexion stratégique.

Face à la densification normative, à l'accélération technologique et à la pression compétitive, les organisations doivent mieux articuler le rôle de leurs instances, clarifier les responsabilités et renforcer le dialogue avec les parties prenantes. Ces évolutions interrogent directement la capacité des Conseils à soutenir une trajectoire durable de performance, de résilience et de confiance.

Cyber et Gouvernance

La recrudescence des attaques cyber est constatée par tous. Elles sont désormais identifiées comme une priorité majeure pour les dirigeants, comme le confirme notamment l'étude *KPMG CEO Outlook*. Les participants rappellent la diversité et la complexité des modes opératoires, en citant notamment les attaques par déni de service, qui visent à saturer un site jusqu'à le rendre indisponible, ainsi que les vols de données, particulièrement déstabilisants pour le fonctionnement des entreprises. Dans ce contexte, la discussion met en avant l'ampleur du risque cyber, la difficulté à apprécier la maturité réelle des groupes face à ce périmètre très large, ainsi que les enjeux de supervision par les instances de gouvernance.

Une supervision portée d'abord par les comités d'audit

La question de la maturité des groupes face au risque cyber et des modalités de sa supervision est soulevée.

Les participants indiquent que ce sujet est, le plus souvent, traité au niveau des comités d'audit, avec des points réguliers permettant de présenter les dispositifs déployés en interne ainsi que les couvertures d'assurance associées, dans une logique où le renforcement des capacités internes peut contribuer à limiter le coût de l'assurance. Ils ont également rappelé que l'exposition au risque varie fortement selon les activités et qu'elle suppose, pour être correctement appréhendée, de s'appuyer sur des analyses précises de vulnérabilité.

Un témoignage a par ailleurs mis en lumière la place croissante accordée à ces enjeux au sein du Conseil, avec des interventions régulières des responsables de la sécurité informatique afin d'exposer les niveaux de protection en place et de donner des éléments de réassurance, sans jamais pouvoir promettre une protection absolue. Les participants ont ainsi rappelé que celle-ci n'existe pas, en particulier lorsque l'entreprise est confrontée à des attaques pouvant être revendiquées ou soutenues par des acteurs étatiques ou assimilés, dont les capacités excèdent parfois le seul registre des défaillances techniques internes.



Une course permanente entre renforcement des défenses et sophistication des attaques

La poursuite du débat établit que le risque cyber est désormais suivi non seulement par les comités d'audit, mais aussi par les comités des risques ou les comités d'audit « et des risques ». Plusieurs participants relèvent un constat récurrent : à mesure que les entreprises renforcent leurs dispositifs, les attaquants progressent eux aussi, souvent plus vite encore, ce qui nourrit le sentiment d'une course permanente pour rester au niveau. Cette dynamique se traduit par une hausse continue des budgets consacrés à la cybersécurité, ainsi que des coûts d'assurance. Les participants soulignent en outre l'importance de la solidarité interentreprises lorsqu'un incident survient, tant pour le partage d'expérience que pour l'appui opérationnel.

Il est également rappelé que le risque cyber figure désormais de manière récurrente à l'agenda des instances de gouvernance, avec une conviction largement partagée : la question n'est plus tant de savoir « si » une attaque surviendra que « quand » elle surviendra. Dans cette perspective, les débats insistent sur la nécessité d'aborder le sujet avec humilité et de s'assurer de l'existence de plans de réponse clairement établis, intégrant notamment les mécanismes d'alerte, les chaînes de décision, les mesures d'action et de réaction, ainsi que l'activation éventuelle d'une cellule de crise. Si les technologies employées par les attaquants gagnent en sophistication, les participants estiment néanmoins que des leviers de défense existent, à condition de s'inscrire dans une démarche continue de prévention, de formation et de sensibilisation.

Les discussions rappellent enfin que certaines attaques s'inscrivent dans le temps long, avec des intrusions discrètes d'espions pouvant précéder de plusieurs mois le passage à l'acte. Cette réalité renforce l'importance des dispositifs de détection précoce et de la capacité des organisations à réagir dès l'apparition d'une anomalie.

Le facteur humain et la culture cyber au cœur de la prévention

Les échanges soulignent que la sensibilisation, la formation et, plus largement, la dimension culturelle constitue un volet essentiel de la maîtrise du risque cyber, qui ne peut être appréhendé sous le seul angle technique. Les participants rappellent que le facteur humain demeure au premier rang des vulnérabilités, y compris dans des périodes particulièrement propices aux intrusions, comme celle des fêtes de fin d'année. Il est toutefois relevé que cette exposition, parce qu'elle est inhérente au fonctionnement des organisations, n'exclut nullement la mise en place de processus adaptés permettant de prévenir les incidents ou d'en détecter les signes précurseurs.

Il est également observé que les risques de divulgation d'informations sensibles concernent aussi des secteurs auxquels on ne les associe pas spontanément. À cet égard, l'exemple du secteur hospitalier pendant la période du Covid est cité pour illustrer l'attractivité particulière de certaines activités pour les attaquants, notamment lorsque la pression opérationnelle et l'impact potentiel d'une interruption d'activité rendent la menace de rançon particulièrement efficace.



Des usages de l'IA à encadrer selon la sensibilité des environnements

Les débats mettent par ailleurs en évidence une approche nuancée des usages de l'intelligence artificielle. Les participants indiquent que, pour certains processus ou certaines typologies de données, le recours à un agent IA peut être écarté lorsque le niveau de dépendance créé apparaîtrait excessif, notamment s'il ne permettrait pas de reconstituer les données ou de rétablir l'activité dans des délais acceptables en cas d'incident majeur ou de nécessité de coupure des systèmes. Il est néanmoins rappelé que l'enjeu cyber ne réduit pas, en soi, le potentiel de l'IA sur d'autres périmètres ou catégories de données, dès lors que les conditions de sécurité sont maîtrisées.

Plusieurs exemples concrets illustrent cette logique de cloisonnement et de sécurisation des usages. Il est ainsi indiqué que, dans certains environnements sensibles, comme la conduite de réacteurs nucléaires, une séparation stricte est maintenue entre les systèmes opérationnels et les systèmes de gestion de l'entreprise. De même, un participant explique qu'après avoir constaté que les requêtes formulées par les collaborateurs dans des outils d'IA pouvaient exposer des

informations internes à l'extérieur, son organisation a très rapidement déployé une plateforme interne sécurisée, puis interdit le recours à d'autres solutions que cette IA interne, conçue pour garantir qu'aucune donnée ne sorte de l'environnement maîtrisé de l'entreprise.

Les participants relèvent enfin que l'IA peut également constituer un levier utile d'assistance, notamment dans les environnements industriels, pour aider à l'interprétation de certains événements ou alertes de fonctionnement d'une usine par exemple. Ils rappellent, dans le même temps, l'importance des exercices de simulation de crise, avec l'exemple d'un exercice annuel organisé au niveau du comité exécutif d'un groupe international, certains administrateurs ayant d'ailleurs déjà été confrontés à ce type de situation dans le cadre de mandats antérieurs.

Face aux cyber-risques, le Conseil doit veiller à la préparation sans se substituer à la gestion de crise

La capacité de l'entreprise à tenir sans déclencher immédiatement son plan de réponse constitue un point d'attention central, dans la mesure où elle dépend directement de la nature de l'attaque, de son ampleur et de ses conséquences financières et opérationnelles.

Les participants relèvent, dans ce contexte, que le rôle du Conseil n'est pas de se substituer aux opérationnels dans la gestion technique de la crise, mais de s'assurer que ceux-ci sont effectivement en ordre de bataille pour réagir et que les dispositifs de réponse ont bien été prévus en amont.

Certains participants sont quant à eux d'avis qu'un exercice de crise conduit au niveau du Conseil n'apparaît pas nécessairement comme le format le plus pertinent. En revanche, tous s'accordent à dire que le Conseil doit être en mesure d'apprécier les impacts potentiels d'une cyberattaque, d'interroger la solidité des dispositifs

de préparation et de vérifier que l'organisation dispose des compétences adéquates pour faire face à un incident majeur. Les participants rappellent à cet égard qu'un Conseil n'a pas vocation à être expert de la cyber, mais qu'il lui revient de s'assurer que les bonnes expertises sont en place, que les scénarios de réaction sont définis et que les principaux indicateurs de pilotage sont suivis, parmi lesquels le niveau des investissements consacrés à la cybersécurité, utilement mis en perspective au regard de références de marché.

Les débats mettent également en avant l'intérêt des campagnes de faux phishing comme outil de sensibilisation. Il est rappelé que leur objectif n'est pas seulement de tester les collaborateurs, mais d'ancrer des réflexes opérationnels concrets, tels que la vérification de l'adresse de l'expéditeur, l'évitement des liens suspects et le recours direct aux sites concernés plutôt qu'aux liens intégrés dans les messages



Des menaces en forte hausse dans un cadre réglementaire qui se renforce

Face à la forte progression des fraudes, et la rentabilité économique certaine de ces opérations (une étude l'a estimée à M€10 par jour), certains participants rappellent que le coût quotidien des atteintes à la cybersécurité peut atteindre des montants considérables pour les organisations visées. Il est réaffirmé, dans ce contexte, que le versement de rançons ne constitue pas une réponse souhaitable, dès lors qu'il contribue à alimenter durablement ces écosystèmes criminels, parfois soutenus ou tolérés par des États qualifiés de hostiles.

Les membres du Cercle rappellent également qu'il demeure difficile de disposer d'un véritable étalon de mesure de la maturité des groupes sur ces sujets, compte tenu de l'étendue du risque et de l'hétérogénéité des situations. Ils relèvent par ailleurs l'importance des évolutions réglementaires en cours, notamment avec la mise en œuvre de la directive NIS 2 (Network and Information Security), publiée au Journal Officiel de l'Union européenne en décembre 2022, qui renforce les obligations de sécurisation sur un certain nombre de périmètres critiques, y compris au travers de la sous-traitance, et prévoit un régime de sanctions assis sur le chiffre d'affaires mondial. L'impact du passage de NIS 1 à NIS 2 est, à cet égard, identifié comme un sujet de vigilance particulier.

Il est enfin souligné que l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) s'inscrit avant tout dans une logique de prévention et d'accompagnement. Plusieurs intervenants mettent en avant l'approche d'un régulateur qui cherche d'abord à aider les organisations touchées, notamment par des audits ou des interventions en soutien des victimes de cyberattaques plutôt qu'à les appréhender sous un angle uniquement répressif.

Une acculturation du Conseil encore entravée par un discours trop technique

On relève ensuite la nécessité, pour les responsables informatiques et cybersécurité, d'adopter un discours plus pédagogique à l'égard des instances de gouvernance..

Selon plusieurs participants, ces interventions demeurent souvent trop techniques, trop chargées en jargon ou en acronymes insuffisamment explicités, ce qui peut nuire à la bonne compréhension des administrateurs. Il est ainsi rappelé que ces temps d'échange avec le Conseil ont d'abord une vocation d'acculturation et de pédagogie, davantage que de technicité, afin de permettre aux administrateurs de se familiariser progressivement avec les notions essentielles.

Également, les entreprises restent généralement très discrètes sur le nombre d'attaques auxquelles elles font face. Il est toutefois suggéré qu'une communication davantage centrée sur les tentatives déjouées ou les attaques absorbées pourrait constituer un indicateur utile pour apprécier le niveau d'exposition et la résilience des organisations. À cet égard, il est rappelé qu'une étude du ministère de l'Intérieur publiée en 2024 fait état d'environ 400 000 attaques numériques par an, en hausse de 74 % sur cinq ans, ce qui illustre l'ampleur croissante du phénomène.



Des infrastructures essentielles particulièrement exposées

Les débats mettent en évidence la vulnérabilité particulière de certains secteurs essentiels, notamment l'eau, l'énergie, les télécommunications et les transports, pour lesquels les enjeux de continuité d'activité revêtent une dimension stratégique. L'exemple des Jeux olympiques de 2024 est cité à ce titre, avec la prise en compte de scénarios touchant les infrastructures de distribution d'eau et la nécessité d'anticiper, entre opérateurs, des solutions de continuité ou de relais.

Plusieurs intervenants soulignent enfin l'intérêt d'adopter, dans l'analyse du risque, le point de vue des attaquants eux-mêmes, en s'interrogeant sur les cibles ou les actions susceptibles de provoquer les dommages les plus importants, ou de susciter la plus forte exaspération de l'opinion publique. Il est, dans le même temps, rappelé que certains groupements de hackers peuvent être soutenus, voire financés, par des États dans une logique de déstabilisation d'autres États, ce qui confère à certaines attaques une portée qui dépasse largement le seul cadre de la criminalité opportuniste.

Le calcul quantique fait émerger une menace encore incertaine

Les débats s'orientent ensuite sur le risque que ferait peser, à terme, le calcul quantique sur les dispositifs de chiffrement. Les participants s'interrogent sur le degré de prise en compte de ce sujet par les entreprises et relèvent le caractère à la fois émergent, systémique et encore difficilement appréhendable de cette menace. Certains indiquent que, si un tel risque devait se matérialiser à grande échelle, il viserait probablement d'abord des cibles étatiques ou stratégiques avant les entreprises de plus petite taille. Il est également souligné que, à ce stade, les plans d'action et les parades demeurent encore peu lisibles, ce qui nourrit une forme d'incertitude sur les réponses concrètes à apporter.

L'IA transforme déjà les organisations et interpelle la gouvernance

Les débats s'élargissent, dans ce prolongement, aux effets plus vastes de l'intelligence artificielle sur les organisations et sur la gouvernance. Plusieurs participants relèvent que les Conseils ne sont pas encore suffisamment informés des incidences de l'IA sur les processus opérationnels, ni des transformations qu'elle pourrait induire dans les trajectoires d'apprentissage et de montée en compétence des plus jeunes collaborateurs, dès lors que certaines tâches formatrices seraient partiellement ou totalement automatisées.

Au-delà des enjeux d'efficacité, l'IA soulève des problématiques éthiques et sociales majeures

Les participants soulignent également que les enjeux liés à l'IA ne se limitent pas à la performance ou à l'efficacité, mais embarquent aussi des questions éthiques majeures, notamment dans le domaine des ressources humaines ou dans le traitement de dossiers à caractère social. L'exemple du secteur de l'assurance est cité pour illustrer les dérives potentielles qu'un usage insuffisamment encadré pourrait entraîner, lorsqu'un agent d'IA serait amené à exploiter l'historique d'un salarié, voire certaines données particulièrement sensibles comme ses antécédents génétiques, pour fonder une décision défavorable, indépendamment de sa situation réelle.

Enfin, les échanges font émerger une interrogation plus large sur l'usage du temps potentiellement libéré par l'IA. Au-delà des gains de productivité attendus, les participants s'interrogent sur la manière dont ce temps pourrait être réalloué, qu'il s'agisse d'intensifier le travail sur les tâches restantes ou, plus largement, de repenser l'organisation du travail et la répartition des contributions au sein de l'entreprise.

ESG et Gouvernance

Un cadre réglementaire en évolution, mais des obligations inchangées à court/moyen terme

Les échanges rappellent d'abord que la directive en cours d'évolution doit être transposée avec une application désormais envisagée à compter de 2027, sur la base de nouveaux seuils et d'une simplification annoncée des ESRS. Il est toutefois souligné que, pour les exercices 2025 et 2026, le référentiel demeure inchangé, ce qui conduit les entreprises à poursuivre leurs travaux dans un cadre qui, à ce stade, reste stable.

Les participants relèvent par ailleurs que la mise en œuvre de la double matérialité conduit, en France, à identifier un nombre d'IROs souvent élevé, parfois perçu comme supérieur à celui observé dans d'autres pays. Dans ce contexte, les échanges posent la question de l'état d'avancement réel des entreprises sur ces travaux ainsi que du rôle que les administrateurs doivent jouer dans leur supervision.

Un premier exercice finalement absorbé, malgré les inquiétudes initiales

Il est également observé que la première année de mise en œuvre a suscité de fortes inquiétudes, mais que les entreprises sont, dans l'ensemble, parvenues à produire l'exercice demandé, ce qui contribue aujourd'hui à une forme d'apaisement et à un recul de la pression ressentie. Plusieurs participants soulignent néanmoins un contraste entre ce tassement et le fait que, dans d'autres enceintes de gouvernance, les priorités des dirigeants semblent déjà se déplacer, notamment vers l'intelligence artificielle, désormais placée au premier rang dans l'étude CEO Outlook.

Un contexte moins prescriptif et un recentrage sur l'essentiel

Les débats font également ressortir un infléchissement plus général du contexte, plusieurs participants relevant que les proxy advisors ont nettement atténué leurs positions sur ces sujets. Il est aussi suggéré qu'au-delà des contraintes réglementaires, un certain nombre d'acteurs considèrent désormais, à titre plus personnel, avoir déjà beaucoup fait en matière d'ESG.

Enfin, les échanges mettent en évidence une forme de mouvement inverse dans l'approche de la matérialité. Là où les premiers exercices ont parfois conduit à retenir un nombre élevé de sujets, une tendance semble désormais se dessiner en faveur d'un recentrage sur un nombre plus limité de priorités, de l'ordre de trois ou quatre enjeux considérés comme véritablement essentiels.



Trop d'IROs nuisent à la lisibilité et à la capacité de pilotage

La suite des échanges consiste à illustrer très concrètement la tension entre l'ambition initiale des exercices de double matérialité et la volonté, désormais plus affirmée, de concentrer le reporting sur un nombre d'enjeux réellement pilotables. Plusieurs participants relèvent qu'un nombre trop élevé d'IROs nuit à la lisibilité comme à la capacité de suivi effectif par les instances dirigeantes, certains indiquant qu'au-delà même d'une quinzaine d'objectifs, l'exercice devient déjà difficile à piloter dans la durée. Il est ainsi souligné qu'une forme de discipline dans la hiérarchisation des priorités s'impose, y compris lorsque les travaux préparatoires conduiraient spontanément à élargir encore le périmètre des sujets retenus.

Les participants rappellent toutefois que ce mouvement de recentrage ne remet pas en cause les actions de fond engagées par les entreprises, notamment en matière de décarbonation, de sobriété dans l'usage des ressources ou de transformation des modèles opérationnels. En revanche, plusieurs intervenants estiment que le niveau de détail du reporting a parfois dépassé ce qui est utile, créant une impression de sur-reporting, en particulier sur le terrain de la communication extra-financière.

Les revers d'une transparence accrue à l'ère de la data et de l'IA

Cette évolution s'accompagne d'une réflexion plus critique sur la notion même de transparence. Là où une communication très étendue pouvait auparavant être perçue comme un signal positif par le marché ou par certaines parties prenantes, plusieurs participants soulignent qu'elle peut désormais accroître l'exposition au risque, notamment dans un contexte marqué par l'essor de l'intelligence artificielle et des capacités de collecte, d'agrégation et d'exploitation automatisée des données publiées. Il est, dans ce cadre, indiqué que certaines entreprises se montrent désormais plus réservées face aux demandes de communication de données supplémentaires, dès lors que toute information diffusée est susceptible d'être réutilisée, sortie de son contexte ou retournée contre elles.

Des méthodologies encore discutées dans un contexte international hétérogène

Les débats font également ressortir des interrogations sur la robustesse de certains calculs ou indicateurs mobilisés dans les exercices ESG, plusieurs intervenants exprimant des réserves sur leur degré réel de scientificité, en particulier sur certains postes complexes comme le scope 3. Plus largement, les participants relèvent le décalage croissant entre l'approche européenne, qui demeure fortement engagée sur ces sujets, et celle observée aux États-Unis, où ces thématiques semblent faire l'objet d'un rejet beaucoup plus marqué.

Des enjeux ESG qui restent profondément ancrés dans la réalité économique

Pour autant, il est rappelé que certaines problématiques au cœur des démarches ESG, en particulier la raréfaction des ressources et les effets du dérèglement climatique, ne relèvent nullement d'une construction théorique. Les participants citent notamment les secteurs agricoles, dans lesquels les perturbations des cycles de production rendent ces enjeux particulièrement tangibles.

Une deuxième année encore incertaine, sans remise en cause des travaux engagés

Enfin, plusieurs intervenants soulignent l'incertitude entourant la deuxième année de mise en œuvre de la CSRD. S'il existe une attente quant à l'évolution des pratiques, il est indiqué que les entreprises n'envisagent pas, pour autant, de reprendre leurs travaux pour revenir en arrière ou supprimer des informations déjà produites, ce qui plaide plutôt en faveur d'une stabilisation pragmatique des approches.

Une articulation plus nette entre comité ESG et comité d'audit

Les échanges portent ensuite sur l'évolution du partage des rôles entre comité ESG ou RSE et comité d'audit. Plusieurs participants indiquent que des réunions communes entre ces deux instances sont désormais organisées dans certains groupes, par exemple à raison de deux fois par an, notamment au moment du lancement de l'exercice. Il est souligné que le comité ESG intervient davantage sur les travaux de fond, qu'il s'agisse du cadrage, des études ou des plans d'action, tandis que le comité d'audit intervient dans un second temps, avec une attention particulière portée à la fiabilité des données, à la robustesse des méthodologies et à la comparabilité des informations produites. Cette répartition des responsabilités est globalement présentée comme cohérente.

Le contrôle interne extra-financier devient un enjeu central de supervision

L'importance de la supervision de l'efficacité du dispositif de contrôle interne appliqué à l'extra-financier est soulignée. Ce sujet est présenté comme central, dans un contexte où les groupes sont encore jugés peu matures sur ces enjeux. Il est rappelé que cette supervision entre pleinement dans les missions du Conseil, tout en appelant une montée en puissance progressive, adaptée au degré de maturité des organisations et à leurs priorités opérationnelles.



Des attentes fortes vis-à-vis des auditeurs dans un cadre encore en stabilisation

Les participants évoquent également les attentes à l'égard des auditeurs dans ce nouveau cadre. Il est relevé que ceux-ci ont, dans l'ensemble, anticipé les évolutions en cours, tandis qu'une tendance semble se dessiner, dans certains cas, en faveur d'un rapprochement des instances compétentes, voire d'un comité unique, les entreprises éprouvant parfois des difficultés à traiter simultanément les sujets relevant de l'audit et ceux relevant de l'ESG dans des cadres séparés.

Bien que la majorité des participants notent une amélioration lors de ce deuxième exercice par rapport à la première année, certaines réserves sont encore exprimées : certains participants relèvent le sentiment que les auditeurs ont parfois pu aller trop loin, soit pour se prémunir contre leur propre risque, soit dans une logique perçue comme excessivement extensive. Il est toutefois aussitôt rappelé que ce cadre était nouveau pour l'ensemble des parties prenantes et que la pression exercée par les autorités publiques, notamment sur la formation des équipes, ainsi que le contexte de forte vigilance externe, y compris de la part de certaines ONG, ont contribué à durcir les approches.

Dans ce contexte, les diligences engagées visaient avant tout à s'assurer que les travaux réalisés répondaient bien aux exigences posées.

Un traitement parfois trop spécialisé, au risque d'une implication tardive des Conseils

Enfin, plusieurs participants estiment que ces sujets ont parfois été laissés, tant du côté des auditeurs que de celui de la gouvernance, entre les mains de spécialistes qui ont pu en accentuer la portée ou la technicité, au risque d'un traitement trop tardif par les Conseils. Il est ainsi relevé que, dans de nombreux cas, les instances de gouvernance n'ont pas disposé suffisamment tôt de la matière nécessaire pour réagir utilement ou infléchir les travaux en temps utile.

La cohésion du Conseil et la formation conditionnent son efficacité collective

Sur ce sujet comme sur beaucoup d'autres, la qualité de la « chimie » du Conseil constitue un facteur déterminant de son efficacité collective. Il est relevé que les situations de crise peuvent, selon les cas, soit renforcer cette cohésion, soit au contraire faire apparaître ou accentuer des fragilités dans le fonctionnement du Conseil. Dans cette perspective, plusieurs participants indiquent que les exercices d'évaluation du Conseil peuvent utilement faire remonter certains de ces points.

Les participants rappellent également l'importance croissante des besoins de formation sur des sujets tels que l'ESG, la cybersécurité et l'intelligence artificielle, qui appellent des ressources, des compétences et des expériences spécifiques. Il est toutefois observé que les formations collectives trouvent parfois leurs limites, en raison de niveaux de maîtrise et d'appétences très hétérogènes au sein des conseils.

Plusieurs intervenants soulignent, à cet égard, l'intérêt de formations ciblées et individualisées lorsque le besoin est exprimé. Dans de telles situations, les entreprises peuvent se montrer très réactives pour financer rapidement la formation la plus adaptée, cette approche étant perçue comme l'un des moyens les plus efficaces de faire progresser le niveau global du conseil.

Les participants estiment en outre que l'identification des besoins de formation devrait être davantage intégrée aux questionnaires d'évaluation du Conseil.

Un exemple est cité pour illustrer la nécessité d'accompagner les administrateurs sur les sujets qu'ils maîtrisent moins. Une administratrice référente sur les questions ESG, disposant par ailleurs d'une expérience reconnue, ne maîtrisait pas initialement certains fondamentaux financiers lors de sa première séance de Conseil. Un temps de formation spécifique lui a alors été consacré afin de lui permettre d'acquérir les bases nécessaires. Les échanges soulignent, à travers cet exemple, qu'il est essentiel de pouvoir dire que l'on ne sait pas ou que l'on ne comprend pas, sans que cela soit perçu négativement.

Enfin, il est essentiel de permettre aux membres les moins à l'aise sur certains sujets de rejoindre le niveau collectif, le Conseil devant être appréhendé avant tout comme une intelligence collective.

Le Board Leadership Center (BLC)

Accompagne les acteurs de la gouvernance dans :

- L'identification des enjeux clés de la gouvernance
- Le décryptage de l'actualité
- Le diagnostic des pratiques du Conseil
- L'acquisition de nouvelles compétences
- Le partage de bonnes pratiques

Offre un espace de réflexion et d'échanges dédié aux acteurs de la gouvernance, en mettant à leur disposition :

- Une équipe d'experts en **gouvernance**, conformité et ESG, s'appuyant sur le conseil scientifique de KPMG Avocats
- Un mode de **communication multiforme** : publications, émissions de radio, ateliers en one-to-one, conférences, cercle entre pairs...
- Un accès aux pratiques de **gouvernance internationales**, via le réseau mondial des BLC de KPMG

Contactez-nous

Nicolas de Luze
Associé, Head of BLC France
T : +33 (1) 55 68 90 49
E: ndeluze@kpmg.fr

Stella Vitchevian
Associée, BLC France et Global Assurance
T : +33 (1) 55 68 68 30
E: svitchevian@kpmg.fr

En savoir plus →

kpmg.fr



Les informations contenues dans ce document sont d'ordre général et ne sont pas destinées à traiter les particularités d'une personne ou d'une entité. Bien que nous fassions tout notre possible pour fournir des informations exactes et appropriées, nous ne pouvons garantir que ces informations seront toujours exactes à une date ultérieure. Elles ne peuvent ni ne doivent servir de support à des décisions sans validation par les professionnels ad hoc. KPMG S.A. est membre français de l'organisation mondiale KPMG constituée de cabinets indépendants affiliés à KPMG International Limited, une société de droit anglais (« private company limited by guarantee »). KPMG International et ses entités liées ne proposent pas de services aux clients. Aucun cabinet membre n'a le droit d'engager KPMG International ou les autres cabinets membres vis-à-vis des tiers. KPMG International n'a le droit d'engager aucun cabinet membre.

© 2026 KPMG S.A., société anonyme d'expertise comptable et de commissariat aux comptes, membre français de l'organisation mondiale KPMG constituée de cabinets indépendants affiliés à KPMG International Limited, une société de droit anglais (« private company limited by guarantee »). Tous droits réservés. Le nom et le logo KPMG sont des marques utilisées sous licence par les cabinets indépendants membres de l'organisation mondiale KPMG