Governance Institute of Australia

Gestion des risques pour les administrateurs :

Un guide

Institut de gouvernance d'Australie 2022

Table des matières

À propos de nous

Le Governance Institute of Australia, association nationale de membres, défend une communauté de plus de 43 000 professionnels de la gouvernance et de la gestion des risques, en dotant nos membres des outils nécessaires pour améliorer la gouvernance au sein de leur organisation. Nous adaptons nos ressources aux membres des secteurs cotés, non cotés et à but non lucratif, et nous veillons à ce que la voix de nos membres soit entendue haut et fort. En tant que seul fournisseur australien d'accréditation en gouvernance agréée, nous proposons une gamme de cours de courte durée, de certificats et d'études de troisième cycle pour contribuer à approfondir les connaissances et l'éducation de la profession en pleine croissance de la gouvernance et de la gestion des risques. Nous gérons un solide programme de leadership éclairé, de projets de recherche et de publications d'actualités et nous nous appuyons sur notre adhésion au Chartered Governance Institute pour surveiller les tendances et les défis mondiaux émergents afin de garantir que nos membres sont préparés. Nos membres savent que la gouvernance est au cœur de chaque organisation - et en ces temps tumultueux, qu'une bonne gouvernance est plus importante que jamais.

Ce que couvre ce guide

Cette ressource a été élaborée par le Governance Institute of Australia dans le cadre de son engagement à promouvoir une bonne gouvernance et une bonne gestion des risques. Elle est conçue pour être une ressource pratique destinée à aider les administrateurs australiens de tous les secteurs.

Son objectif est d'aider les conseils d'administration à intégrer et à améliorer leur surveillance des cadres de gouvernance et de gestion des risques. Cela aidera les organisations à atteindre leur objectif stratégique, en fournissant aux conseils d'administration les informations dont ils ont besoin et en garantissant que tous les employés s'approprient en permanence les risques en lien avec la réalisation des objectifs stratégiques. Il n'a pas pour objectif de conseiller les administrateurs sur la manière de créer un système de gestion des risques d'entreprise ou un processus de gestion des risques technique dirigé par la direction – ces éléments sont davantage adaptés au développement par la direction.

L'édition originale du guide a été publiée sous le titre Gestion des risques : Manuel à l'intention des administrateurs en 2016. Cette édition révisée est publiée en 2022.

Remerciements

Le Governance Institute reconnaît la contribution de Judith Fox FGIA, auteur de la première édition de ce guide.

Glossaire

ACNC signifie la Commission australienne des organisations caritatives et à but non lucratif qui réglemente les organisations caritatives.

ASIC signifie Australian Securities and Investments Commission, l'organisme de réglementation des entreprises, des marchés, des services financiers et du crédit à la consommation.

APRA signifie l'Australian Prudential Regulated Authority, l'organisme de régulation des banques, des assurances et des fonds de pension.

La règle de jugement commercial détermine la capacité des administrateurs à se fonder sur l'article 180(2) de la Loi sur les sociétés en ce qui concerne leur obligation d'agir avec soin et diligence en vertu de l'article 180(1) de la Loi sur les sociétés.

Loi sur les sociétés désigne la Loi sur les sociétés de 2001.

Principes et recommandations de gouvernance d'entreprise désigne les Principes et recommandations de gouvernance d'entreprise, 2019, 4e édition, ASX Corporate Governance Council.

ESG signifie environnemental, social, gouvernance.

Le zéro net ou zéro émission nette signifie atteindre un équilibre global entre les émissions de gaz à effet de serre produites et les émissions de gaz à effet de serre éliminées de l'atmosphère.1

La sphère de sécurité désigne une disposition légale visant à réduire ou à éliminer la responsabilité légale ou réglementaire dans certaines situations, à condition que certaines conditions soient remplies, notamment l'article 588G de la Loi sur les sociétés.

[1] Voir le Conseil Climat.

Avant-propos

Les administrateurs ont le devoir fiduciaire d'agir dans le meilleur intérêt de l'entreprise. Afin de s'acquitter de leurs obligations, les administrateurs doivent connaître et évaluer correctement la nature et l'ampleur des risques auxquels l'entité est confrontée.

Un cadre intégré de gouvernance et de gestion des risques est essentiel à la fois pour que le conseil d'administration puisse prendre des décisions éclairées et pour s'adapter aux changements de l'environnement dans lequel évolue l'organisation. Ce guide est resté l'une de nos ressources les plus demandées depuis sa première publication en 2016. Les récents événements d'entreprise de grande envergure, où la gestion des risques a souvent été soulignée comme un échec, nous rappellent avec force l'importance de la surveillance de la gestion des risques par le conseil d'administration.
La récente pandémie mondiale, avec ses impacts sur les chaînes d'approvisionnement et son accélération de nouveaux modèles de travail et de menaces à la cybersécurité, a fondamentalement remis en question la manière dont les conseils d'administration identifient, atténuent et surveillent les risques.

Les actionnaires, les investisseurs et les membres attendent de plus en plus des conseils d'administration qu'ils démontrent et divulguent publiquement une surveillance efficace de la gestion des risques, en particulier en ce qui concerne les risques climatiques et cybernétiques. Les entités du secteur public dotées d'un conseil d'administration sont également soumises à un examen de plus en plus approfondi de la part des parlements, des ministres, des ministères, des organismes d'intégrité, des médiateurs et des vérificateurs généraux. Il est de plus en plus reconnu que la capacité du conseil d'administration à gérer et à divulguer efficacement les risques a un impact sur un plus large éventail de parties prenantes, notamment les employés et les communautés dans lesquelles les organisations opèrent. Ce niveau accru de surveillance publique est illustré par une enquête de 2020 du Governance Institute qui a révélé que 60 % des professionnels du risque considèrent que l'atteinte à la marque ou à la réputation figure parmi les cinq principaux risques auxquels les organisations sont confrontées dans un avenir immédiat.2

Ce guide pratique a pour objectif de fournir aux administrateurs, nouveaux, actuels et futurs, les outils nécessaires pour s'acquitter de leurs obligations. Il ne se résume pas à une simple liste de règles à respecter ou à une longue liste de réglementations : il vise plutôt à susciter des questions stimulantes dans l'esprit des administrateurs individuels et à susciter un débat sain autour de la table du conseil d'administration.

Ce guide est destiné à aider les administrateurs de tous les secteurs. Il est indispensable de le lire, que vous soyez administrateur d'une société cotée ou non, d'une organisation à but non lucratif ou d'une entité du secteur public dotée d'un conseil d'administration, et quelle que soit sa taille.

Depuis la première publication de ce guide, les administrateurs australiens et leurs organisations ont indéniablement gagné en maturité face aux risques. Les conseils d'administration sont devenus de plus en plus systématiques et ont adopté des processus de gestion des risques plus structurés.
Elles bénéficient d'une évaluation plus consciente des risques inhérents à leurs opérations quotidiennes, aidée par les progrès des techniques et technologies de gestion des risques, même si des différences sectorielles subsistent. L'impact des commissions royales sur les services financiers et les soins aux personnes âgées et l'enquête prudentielle de l'APRA sur la CBA ont également conduit à une attention accrue portée à la gestion des risques.

L'enjeu est désormais de poursuivre cette maturation dans d'autres domaines tels que la culture et les risques non financiers, dont la cybersécurité – domaines sur lesquels le guide porte une attention renouvelée.

Cette ressource mise à jour s'appuie sur le travail original de Judith Fox et a été révisée par le Governance Institute avec les précieuses contributions de membres qui sont des praticiens de la gestion des risques, des secrétaires d'entreprise et des membres seniors de la communauté des affaires et à but non lucratif.

Armé de ce guide, un directeur est bien placé pour aborder cet élément essentiel de la bonne gouvernance qui est essentiel au succès de l'organisation.

Megan Devise
PDG

Pauline Vamos
Chaise

[2] Institut australien de gouvernance, rapport d'enquête sur la gestion des risques 2020 2020, p. 32.

Une approche intégrée de la gestion des risques est Au cœur de la bonne gouvernance

Les codes de gouvernance et les régulateurs placent la gestion et la surveillance des risques au cœur de la gouvernance d'entreprise et du rôle du conseil d'administration dans la gestion des organisations, et ce pour de bonnes raisons. Les échecs en matière de gestion des risques sont souvent liés à une faiblesse de la gouvernance, et vice versa.

La gouvernance et le risque doivent être considérés comme liés et intégrés dans un cadre unique.

> La gestion des risques doit être intégrée à la gouvernance dans un cadre unique pour toute organisation supervisée par un conseil d'administration ou un autre organe directeur. Le conseil d'administration doit mettre en place un processus structuré et continu pour identifier, gérer et ré

Qu'est-ce que le risque et la gestion des risques ?

La prise de risque est une caractéristique des organisations : elle fait partie de chaque décision qu'elles prennent. La norme de gestion des risques ISO 31000 2018 définit le risque comme « l'effet de l'incertitude sur les objectifs » et la gestion des risques comme « des activités coordonnées visant à diriger et à contrôler une organisation en ce qui concerne les risques ».3
Le risque englobe les opportunités de création de valeur pour l'organisation (risque de hausse ou d'opportunité) ainsi que les menaces ou dangers présents et à prendre en compte pour garantir que la valeur ne soit pas compromise (risque de baisse), en tenant compte des incertitudes liées aux opportunités comme aux dangers. Les organisations qui gèrent bien le risque peuvent limiter l'impact des menaces et tirer parti des opportunités.

La gestion des risques est essentielle car elle aide les organisations à définir une stratégie, à atteindre leurs objectifs, à prendre des décisions éclairées et à éviter les pertes potentielles. Elle protège également les clients et les parties prenantes vulnérables des impacts néfastes, tels que ceux étudiés par les commissions royales sur les secteurs des services financiers et des soins aux personnes âgées.

Les éléments clés d'un cadre de gestion des risques comprennent :

- évaluer l'appétit et la tolérance de l'organisation pour le risque
- des lignes de responsabilité claires et documentées et la responsabilité de la gestion des risques et des décisions en matière de risques
- un processus documenté permettant d'identifier les types d'événements susceptibles de compromettre la réalisation des objectifs de l'organisation, ainsi que les opportunités de création de valeur
- mettre en place des politiques et des processus pour atténuer les risques identifiés
- surveiller et gérer les risques au fil du temps à un niveau opérationnel
- établir des plans d'urgence pour les événements à risque majeur et les situations d'urgence qui peuvent survenir, et
- évaluer régulièrement l'adéquation du risque cadre de gestion.

L'environnement réglementaire

Bien qu'il ne s'agisse en aucun cas d'un concept nouveau, la gestion des risques fait l'objet d'une attention et d'une activité réglementaire croissantes dans de nombreux domaines. juridictions. L'Australie ne fait pas exception. Aucun secteur n'est à l'abri.

Les administrateurs sont confrontés à un ensemble de plus en plus complexe de réglementations nationales, étatiques et internationales en matière de gouvernance et de gestion des risques, qui comprennent un mélange de régimes obligatoires, volontaires, fondés sur des principes et des règles. Certains secteurs sont plus fortement réglementés que d'autres. Tous les codes et réglementations ne sont pas harmonisés et nombre d'entre eux varient dans leur niveau de détail en matière de gestion des risques.

Ces exigences réglementaires de plus en plus strictes ont été influencées par des événements locaux et mondiaux. Il s'agit notamment des faillites d'entreprises de grande envergure qui ont conduit à la réglementation Sarbanes-Oxley aux États-Unis (2002), de la crise financière mondiale de 2008, de la Commission royale sur les services financiers en Australie (2017-2019), de la Commission royale sur la qualité et la sécurité des soins aux personnes âgées (2018-2021), du consensus croissant sur la science du changement climatique, de l'adoption rapide des technologies numériques, de la pandémie de COVID-19 et des conflits mondiaux.

[3] Normes australiennes, 2018, AS ISO 31000:2018, < https://www.standards.org.au/standards-catalogue/sa-snz/publicsafety/ob-007/as--iso--31000-colon-2018 >.

Qu'est-ce que cette réglementation en évolution rapide L'environnement souligne la responsabilité ultime du conseil d'administration en matière de gestion des risques et l'importance pour les administrateurs d'adopter une perspective intégrée à l'échelle de l'organisation pour la surveillance des risques.

Les obligations réglementaires des administrateurs en matière de gestion des risques comprennent :

- les devoirs des administrateurs en common law, dans la Loi sur les sociétés et en vertu d'autres lois
- les principes de gouvernance d'entreprise de l'ASX et Recommandations pour les sociétés cotées
- Normes, réglementations et directives réglementaires ASIC, APRA et ATO
- la Loi sur la protection des renseignements personnels et les violations de données à signaler au Commissariat du Commissaire australien à l'information
- réglementation émergente autour de la cybersécurité et de la protection des actifs d'infrastructures critiques et des actifs d'importance nationale
- législation sur la protection de l'environnement
- lois anti-discrimination
- lois contre le blanchiment d'argent
- législation sur la dénonciation d'irrégularités
- législation et normes de gouvernance du secteur public applicable aux entités du secteur public
- Législation et réglementation de l'ACNC applicables aux organismes de bienfaisance et à but non lucratif
- législation des États et des territoires applicable aux associations constituées en société
- législation sur la santé et la sécurité au travail et droits des travailleurs droit d'indemnisation.

En d'autres termes, outre leur devoir d'agir dans le meilleur intérêt de l'organisation, les administrateurs ont d'autres obligations légales et fiduciaires. Pour s'acquitter de ces obligations, les administrateurs doivent surveiller attentivement et, le cas échéant, divulguer les risques auxquels l'entité est confrontée.

Les administrateurs des sociétés régies par la Corporations Act bénéficient d'une certaine protection contre la responsabilité personnelle grâce à l'application de la disposition de protection relative aux réclamations pour insolvabilité commerciale et de la règle de l'appréciation commerciale, qui protège les administrateurs contre la responsabilité personnelle pour les mauvaises décisions prises dans l'exercice de leurs fonctions. Toutefois, il est peu probable que ces protections s'appliquent si les administrateurs ne le font pas. prendre des mesures proactives pour s'acquitter de leurs devoirs. Cela souligne la nécessité pour les administrateurs de comprendre et d'assumer leurs devoirs

Il faut prendre très au sérieux la gestion des risques et veiller à ce que les conseils d'administration s'assurent collectivement qu'un cadre de gestion des risques et de gouvernance solide et intégré est en place et continuellement amélioré.

Intérêt des actionnaires et des membres dans la surveillance de la gestion des risques par le conseil d'administration

Dans de nombreuses juridictions, les entités cotées sont censées appliquer les principes et pratiques d'un code de gouvernance en vigueur dans la juridiction concernée ou fournir une explication des raisons pour lesquelles elles ne l'ont pas fait.4 Les investisseurs se tournent vers ces informations pour prendre des décisions concernant le déploiement de leur investissement en capital. Ils sont de plus en plus désireux d'obtenir plus de clarté sur la manière dont les conseils d'administration supervisent la gestion des risques au sein de l'organisation et sur la capacité de l'équipe de direction à exercer un contrôle. Les investisseurs considèrent que la capacité du conseil d'administration à présenter une évaluation équilibrée et compréhensible des performances et des perspectives de l'entité est essentielle pour savoir si un conseil d'administration assume correctement sa responsabilité d'agir en tant qu'agent des actionnaires pour préserver et créer de la valeur en leur nom.

Les membres d'organisations non cotées, bien que ne cherchant pas nécessairement à prendre des décisions sur le déploiement d'un investissement financier, sont tout aussi désireux d'évaluer la capacité du conseil d'administration à :

- définir l'appétence au risque de l'organisation
- superviser le cadre de gestion des risques mis en œuvre par la direction et s'assurer que ce cadre est solide.

Les entités du secteur public dotées d'un conseil d'administration sont créées pour exercer certaines fonctions pour le compte du gouvernement qui ont été approuvées par le parlement responsable et le ministre concerné aura intérêt à ce que le conseil d'administration rende des comptes en ce qui concerne sa surveillance de la gestion des risques au sein de l'entité. Les organismes centraux et de protection de l'intégrité tels que les vérificateurs généraux, les commissions de la fonction publique, les médiateurs, les organismes de lutte contre la corruption et les ministères du Trésor peuvent également avoir un intérêt. Les conseils d'administration des entités du secteur public doivent également tenir compte de l'intérêt des autres parties prenantes, notamment de la communauté, dans la surveillance de la gestion des risques.

[4] En Australie, les règles de cotation de l'Australian Securities Exchange (ASX) exigent la divulgation de la mesure dans laquelle les cadres et pratiques de gouvernance d'entreprise des entités cotées s'alignent ou diffèrent des principes et recommandations de gouvernance d'entreprise, le régime « si non, pourquoi pas ».

Question clé pour les réalisateurs :

- Si votre organisation a fait l'objet d'une plainte royale La Commission ou un autre organisme d'examen externe important pourrait-il identifier les manquements ou les faiblesses de votre cadre de gouvernance et de gestion des risques ?
- Selon vous, comment l'équipe de direction de votre organisation répondrait-elle à la question ci-dessus ?

Répartition des responsabilités

Le rôle du conseil d'administration

La gestion des risques commence et se termine au niveau du conseil d'administration. Il s'agit d'un rôle de surveillance et non d'une implication dans la gestion quotidienne des risques.

Le conseil d'administration a la responsabilité globale de définir la stratégie et le modèle économique de l'organisation ainsi que le niveau de risque correspondant.

La définition d'une stratégie et la gestion des risques sont étroitement liées. Le conseil d'administration définit l'appétence au risque de l'entité, c'est-à-dire la nature et l'ampleur des risques qu'elle est prête à prendre pour atteindre ses objectifs. Le conseil d'administration supervise le cadre intégré de gestion des risques et de gouvernance et s'assure régulièrement qu'il reste solide. Cela implique

mettre en place un processus structuré et continu pour identifier, gérer et répondre aux risques et superviser la mise en œuvre par la direction de la gestion des risques stratégiques et opérationnels.

Il convient de bien délimiter les rôles du conseil d'administration et de la direction. Le conseil d'administration n'est pas un simple « tampon ». Il peut rejeter ou modifier les recommandations de la direction. Le conseil d'administration ne donne pas effet aux éléments opérationnels du cadre. Les administrateurs doivent faire preuve de prudence lorsqu'ils mettent de côté des recommandations fortement exprimées par la direction.

Il peut être approprié pour le conseil d'administration d'intensifier temporairement sa supervision de la direction en réponse à des événements majeurs de gestion des risques ou à des moments cruciaux dans la réalisation des objectifs organisationnels tels que les fusions et acquisitions et les grands projets de transformation numérique.

Administrateurs individuels

Les administrateurs doivent être conscients de leurs responsabilités et de leurs devoirs en matière de gestion des risques. Tous les administrateurs, dès leur entrée en fonction et par la suite, doivent comprendre les activités de l'entité et les risques commerciaux importants auxquels elle est confrontée. Le président

Le conseil d'administration doit régulièrement examiner et convenir avec chaque administrateur de ses besoins en matière de formation et de développement afin de garantir que les administrateurs, en tant que groupe, possèdent et maintiennent les compétences, les connaissances et la familiarité avec l'organisation nécessaires pour remplir efficacement leur rôle au sein du conseil et des comités du conseil.

Le conseil d'administration doit être composé d'un mélange approprié d'administrateurs non exécutifs et exécutifs. Cela implique de disposer d'un nombre suffisant d'administrateurs non exécutifs indépendants qui peuvent remettre en question la direction et lui demander des comptes et représenter les meilleurs intérêts de l'organisation et de ses membres dans leur ensemble plutôt que ceux de chaque individu.

membres ou groupes d'intérêt. Cependant, il incombe à tous les administrateurs, et pas seulement aux administrateurs non exécutifs indépendants, d'exercer un jugement indépendant et actif.

Étant donné le rôle essentiel des comités d'audit, de gestion des risques et des comités du conseil d'administration connexes, il est essentiel que les membres individuels de ces comités consacrent suffisamment de temps et d'attention à leurs devoirs.

Les administrateurs doivent s'assurer qu'ils disposent de suffisamment de temps pour répondre aux obligations de leur rôle. Les administrateurs qui siègent à plusieurs conseils et les comités des risques doivent s'assurer qu'ils disposent de capacités suffisantes, en particulier pendant les périodes de charge de travail intense.

Les administrateurs doivent également réfléchir à la manière dont ils contribuent personnellement à promouvoir une culture du conseil d'administration efficace et respectueuse. Les administrateurs efficaces encouragent une culture du risque au sein du conseil d'administration, équilibrée par la discrétion et le respect.

La durée du mandat peut également être pertinente pour la capacité d'un administrateur à contribuer efficacement à la gestion des risques.
Les principes et recommandations de gouvernance reconnaissent que un mandat prolongé peut constituer un risque pour l'indépendance des administrateurs et la perte d'opportunités d'idées et de perspectives nouvelles.[5]

Délégations d'autorité

La gouvernance de l'ensemble de l'organisation concerne la manière dont l'autorité est exercé et contrôlé au niveau inférieur dans une organisation.
L'autorité passe du conseil d'administration au PDG puis au l'équipe de direction et dans toute l'organisation.

Tous les décideurs de l'organisation doivent comprendre la raison pour laquelle l'autorité est exercée : faciliter la réalisation des objectifs stratégiques de l'organisation (le pourquoi). Tous les décideurs doivent comprendre comment l'autorité est exercée, qui a l'autorité de faire quoi et quelles limites s'appliquent (le comment).

[5] Voir la discussion dans ASX Corporate Governance Council (2019) Corporate Governance Principles and Recommendations, 4e édition, ASX Corporate Governance Council, p. 14. Recommandation 2.3.

Des systèmes de surveillance appropriés devraient être mis en place pour garantir (garantir) que les décisions sont prises de la bonne manière et pour le bon objectif.

Le conseil doit savoir qu'un cadre efficace est en place.
lieu précisant qui est autorisé à prendre quelles décisions et dans quelles circonstances.

Il convient également de mettre en place des pouvoirs délégués complets, articulant clairement à chaque décideur au sein de l'organisation sa capacité à prendre des décisions en rapport avec ses responsabilités et ses devoirs spécifiques. Le cadre de délégation de pouvoirs doit être aligné sur les objectifs stratégiques de l'organisation. La délégation de pouvoirs est une structure clé articulant la tolérance au risque dans une organisation.

La politique de délégation de pouvoirs doit préciser que la définition des délégations de pouvoirs est un élément fondamental d'un cadre de gestion des risques. Il ne s'agit pas d'une politique autonome, mais d'un élément central du cadre de gouvernance d'une organisation, tant au niveau du conseil d'administration qu'au niveau inférieur. Elle fournit un cadre pour la prise de décision et la responsabilisation au sein de l'organisation et doit donc être claire et facile à utiliser pour le personnel.
Une formation appropriée est essentielle pour garantir que le personnel comprenne les limites opérationnelles de sa délégation.

Lors de la définition des délégations de pouvoirs, la direction doit les prendre en compte dans le cadre de la gestion des risques au moyen de tests de scénarios. Cela peut inclure la prise en compte des risques de conséquences imprévues si une autorité particulière est déléguée.

Le conseil d'administration et la direction doivent s'assurer que tous les risques importants, financiers et non financiers, sont couverts par les délégations de pouvoirs. Une faiblesse courante des cadres de délégation de pouvoirs est qu'aucun dirigeant n'est responsable des risques non financiers.

Pour les organisations réglementées par l'APRA, le régime de responsabilité des dirigeants bancaires (BEAR) établit des obligations de responsabilité pour les banques et autres institutions de dépôt autorisées ainsi que pour leurs directeurs et cadres supérieurs.
Le BEAR sera remplacé par le Financial Accountability Regime (FAR). Le FAR étendra les exigences renforcées en matière de responsabilité, de type BEAR, à d'autres entités réglementées par l'APRA et à leurs administrateurs et cadres supérieurs.
objectif de renforcer et d'accroître la responsabilité au niveau individuel et au niveau des entités dans l'ensemble du secteur des services financiers, y compris en ce qui concerne les risques liés aux comportements non financiers.

Comités du conseil d'administration – audit et risque

Le conseil d'administration est responsable en dernier ressort de la supervision de la gestion des risques. Dans l'exercice de cette responsabilité, les conseils d'administration créent souvent des comités qui se concentrent sur des questions particulières. Deux domaines d'intérêt courants sont les suivants :

- surveillance des risques et contrôle interne
- l'intégrité des rapports financiers.

Les manquements perçus par les comités d'audit et de risque ont fait l'objet d'une attention particulière dans l'enquête prudentielle de l'APRA sur la Commonwealth Bank of Australia et dans le rapport final de l'APRA.
Commission royale Hayne.[6] Cela souligne la nécessité de la le conseil d'administration doit accorder une attention particulière à la structure, à la composition et aux fonctions de ces comités, et les administrateurs doivent s'acquitter individuellement de leurs devoirs avec toute l'attention nécessaire.

Comme pour tout comité de direction, le comité d'audit et de gestion des risques doit fonctionner selon une charte ou un mandat écrit qui énonce clairement le rôle, la composition et les responsabilités spécifiques du comité ainsi que les pouvoirs qui lui seront délégués. La composition et les fonctions de ces comités dépendront des circonstances particulières de chaque entité, notamment de sa taille, de sa complexité et de la nature de ses fonctions et de ses opérations. Il est important de réexaminer régulièrement la composition des comités du conseil d'administration pour s'assurer qu'il existe un équilibre approprié des compétences nécessaires à l'exécution de leur travail. Cet examen est généralement effectué chaque année par le président du comité avec l'aide du secrétaire de la société.

Depuis la première édition de ce guide, on observe une évolution progressive vers une séparation entre la gestion des risques et l'audit. L'enquête sur les risques 2020 du Governance Institute a révélé que les comités de risques dédiés étaient plus courants dans les sociétés cotées à l'ASX (40 % des répondants) que dans les grandes entreprises non cotées (27 %) et dans le secteur public (27 %).[7] Cependant, il n'existe toujours pas de consensus sur la question de savoir s'il est préférable d'avoir un comité d'audit et un comité des risques distincts, ou de combiner ces comités. Il est également possible de ne pas avoir de comité des risques dédié, dans la mesure où la gestion des risques relève de la responsabilité de chaque conseil d'administration et de chaque comité du conseil d'administration.

L'exception notable est lorsque la structure du comité est obligatoire. L'APRA exige que les institutions réglementées par l'APRA établissent un comité d'audit du conseil d'administration et un comité de gestion des risques du conseil d'administration.
Comité. Un comité d'audit est obligatoire en Australie pour les 500 premières entreprises en vertu de la règle de cotation ASX 12.7.
Le principe 4 des lignes directrices sur les principes et recommandations de gouvernance d'entreprise recommande à tous les

[6] Voir Prudential Inquiry into Commonwealth Bank of Australia, APRA, 30 avril 2018, pages 16-17.
[7] Rapport d'enquête sur la gestion des risques 2020, Governance Institute of Australia, p. 16.

les entités établissent un comité d'audit, et le principe 7 recommande aux entités cotées d'établir un comité ou

comités pour surveiller les risques, mais ne précise pas qu'il doit être un comité des risques autonome ou combiné avec un

comité d'audit. En revanche, un comité d'audit et de gestion des risques combiné Le comité est mandaté pour tous les départements gouvernementaux et organismes statutaires de la Nouvelle-Galles du Sud.8

Les principaux facteurs qui influencent la structure des comités sont les suivants : les contraintes en termes de ressources, la question de savoir si la combinaison de l'audit et des risques peut apporter de la clarté, en particulier lorsque les principaux risques sont financiers, et si le fait d'avoir des comités distincts permettra de disposer de plus de temps de délibération. Dans le cadre d'une étude sur la surveillance des risques non financiers par les administrateurs, l'ASIC a remis en question ce qu'elle considérait comme des heures de réunion « modestes » pour les comités des risques dans les institutions qu'elle a examinées, qui allaient de 16 à 40 heures par an dans son échantillon.9

De nombreuses entités cotées auront plus d'un comité de direction. responsable de la surveillance des différents éléments de risque, Compte tenu de l'augmentation rapide des cyberincidents pendant la pandémie de COVID-19, de nombreuses organisations examinent quel comité devrait être responsable du risque cybernétique. Certaines organisations incluent le risque cybernétique dans les responsabilités du comité d'audit et de risque, d'autres forment un comité distinct. Quelle que soit l'approche adoptée, le comité responsable doit être convaincu que son organisation est suffisamment préparée pour faire face à ce risque.10

Il est essentiel de clarifier la manière dont les comités du conseil communiquent entre eux et avec le conseil pour garantir

que chaque comité bénéficie des connaissances des autres comités. Les comités d'audit et de risque, lorsqu'ils sont distincts, doivent entretenir une étroite collaboration afin de préserver la cohérence.

En règle générale, un comité des risques du conseil d'administration :

- assure la supervision des activités et conseille le conseil d'administration en relation avec les risques actuels et potentiels futurs et les stratégies de gestion des risques, éventuellement en relation avec un domaine d'activité spécifié
- fournit des recommandations sur l'appétence au risque et tolérance
- surveille la gestion des risques dans le cadre de ses attributions, et
- identifie au conseil les questions relevant de sa compétence pour lesquelles il estime qu'une action ou une amélioration est nécessaire et recommande les mesures à prendre.

Quelle que soit la structure du comité, il ne peut y en avoir qu'un seul. processus de gestion au sein de l'organisation et il devrait

avoir une vision unique et intégrée des risques présentés au conseil d'administration.

Le rôle du management

Il appartient à la direction de recommander, d'exécuter et d'opérer dans le cadre de l'appétence au risque, du cadre et du processus approuvés par le conseil d'administration, conformément à la stratégie du conseil d'administration et sous réserve de sa surveillance.

Les attentes des conseils d'administration concernant l'implication et l'attention des équipes de direction en matière de gestion des risques augmentent.

La direction doit établir des mécanismes pour :

- surveiller l'exposition et les performances en matière de gestion des risques — surveiller l'appétence au risque au niveau organisationnel signifie qu'il doit y avoir une manière claire et définie de faire remonter les résultats de la surveillance des risques de tous les domaines de l'organisation
- approuver la rétention des risques
- faire respecter les tolérances au risque prescrites par le conseil d'administration — une déclaration efficace d'appétence au risque façonnera la manière dont l'organisation est gérée, et
- surveiller et évaluer régulièrement les processus de gestion des risques et en rendre compte au conseil d'administration.

Nommer et remettre en question la direction

Une bonne gouvernance exige une séparation appropriée entre ceux qui sont responsables de la gestion quotidienne d'une organisation et ceux qui sont chargés de superviser sa gestion.

Une surveillance efficace des risques commence par une compréhension mutuelle claire de l'étendue et de la nature des responsabilités du conseil d'administration par rapport à celles de la direction et des autres parties prenantes. L'objectif ultime est que les conseils d'administration aient confiance dans les informations qu'ils reçoivent de la direction et que la direction crée un processus cohérent dans lequel les risques et leurs impacts sont systématiquement identifiés, évalués et traités. L'évaluation des risques pour la réputation et la viabilité à long terme de l'organisation est la responsabilité des deux parties.

L'un des rôles les plus importants d'un conseil d'administration est de sélectionner, de nommer et, si nécessaire, de remplacer le directeur général. Dans de nombreuses organisations, le conseil approuve également la nomination et, si nécessaire, le remplacement d'autres cadres supérieurs. Les conseils d'administration doivent périodiquement évaluer si la direction actuelle a la capacité de gérer efficacement les risques, notamment dans le cadre de la planification de la succession et des politiques de rémunération des dirigeants.

La capacité des administrateurs à porter un jugement indépendant
Il est important de peser sur la prise de décision et de remettre en question les dirigeants. Il s'agit d'empêcher qu'un individu, en particulier le PDG, ne domine un conseil d'administration. Une culture du consensus, dans laquelle les recommandations de la direction ne sont ni remises en question ni contestées, doit être évitée, surtout en période de réussite commerciale apparente. Une telle remise en question repose sur une compréhension claire des risques et des opportunités stratégiques auxquels l'organisation est confrontée.

[8] Trésor de la Nouvelle-Galles du Sud (2020) Politique d'audit interne et de gestion des risques pour le secteur de l'administration générale (TPP20-08), p. 2.
[9] Rapport de surveillance des risques non financiers par les administrateurs et les dirigeants , ASIC Corporate Governance Taskforce, 2019, p. 43.
[10] Voir Cyber Risk Readiness, Response & Ransom : An Audit Committee perspective, The Institute of Internal Auditors Australia 2022.

La Commission royale sur les services financiers a souligné l'importance cruciale pour les administrateurs de demander des comptes à la direction.

> Les conseils d'administration ne peuvent pas fonctionner correctement sans disposer des bonnes informations. Et ils ne peuvent pas fonctionner efficacement s'ils ne remettent pas en question les décisions de la direction.
> Commissaire Kenneth Hayne11

Chef de la direction des risques

Il est de plus en plus courant pour les conseils d'administration de désigner un dirigeant pour diriger le processus de gestion des risques afin de promouvoir la responsabilisation.

Les entités réglementées par l'APRA sont tenues de disposer d'une fonction de gestion des risques désignée et doivent nommer un responsable des risques (CRO) chargé de cette fonction.

Le CRO doit rendre compte directement au PDG et son bureau doit être indépendant de toutes les autres unités commerciales.
Il peut être utile pour le CRO de disposer d'une ligne hiérarchique claire et directe avec l'ensemble du conseil d'administration et/ou le comité d'audit/risque, afin de garantir qu'une « voix » non diluée et non conflictuelle sur les risques soit entendue au niveau du conseil d'administration. Un CRO dédié peut également contribuer à intégrer plus complètement les processus de gestion des risques dans les opérations quotidiennes de l'organisation.

Qu'un CRO soit nommé ou non, les attentes du conseil d'administration en matière d'implication accrue du PDG et de l'équipe de direction et d'attention portée à la gestion des risques augmentent.

Fonction dédiée à la gestion des risques

La taille de l'organisation, la composition de ses activités et sa complexité détermineront si les ressources nécessaires à la mise en œuvre d'une fonction interne de gestion des risques sont suffisantes. Cette unité peut être rattachée à un responsable des risques ou à un autre cadre supérieur.

Une fonction de gestion des risques est chargée de concevoir et de mettre en œuvre le cadre de gestion des risques adapté à l'organisation. En coordonnant la participation de tous les aspects de l'entreprise à la gestion des risques, une fonction de gestion des risques s'appuie sur les informations déjà disponibles. Elle développe également des canaux de communication pour garantir que la stratégie et l'appétence au risque sont au cœur de l'élaboration des stratégies de gestion des risques et que les informations provenant de diverses sources de l'entreprise sont synthétisées pour être communiquées au conseil d'administration. Si l'organisation dispose d'une fonction de gestion des risques et cherche à mettre en œuvre un cadre de gestion des risques d'entreprise, la fonction doit être structurée et avoir pour mandat de remplir son rôle et ses responsabilités.

La fonction de gestion des risques doit être suffisamment proche de l'entreprise pour pouvoir la conseiller correctement, plutôt que d'être hébergée dans un silo séparé. En même temps, la fonction de gestion des risques ne doit pas être « captée » par les fonctions commerciales et doit conserver une indépendance suffisante pour remplir sa fonction d'assurance, remettre en question les décisions des autres unités commerciales et, si nécessaire, faire remonter les préoccupations. Chaque organisation doit décider de l'équilibre approprié entre ces deux aspects de sa fonction. Dans les grandes organisations, ces fonctions peuvent être des rôles distincts et occupés par des personnes différentes, mais ce n'est pas forcément le cas dans les organisations plus petites.

Les dirigeants doivent garder à l'esprit que la gestion des risques remplit à la fois une fonction de contrôle et une fonction stratégique. La gestion des risques est moins efficace dans les organisations où elle fonctionne uniquement comme une fonction de contrôle.

Si l'organisation dispose d'une fonction interne de gestion des risques et une fonction d'audit interne, le conseil d'administration devrait tenir compte de l'interaction entre ces deux fonctions au sein de l'entité.

Question clé pour les administrateurs concernant la fonction de gestion des risques :

- Dans quelle mesure l'équipe de gestion des risques est-elle proche de l'entreprise ? une équipe capable de fonctionner de manière objective ?
- Les termes utilisés sont-ils pertinents et compris par tout le monde dans l'entreprise ?
- La direction conserve-t-elle la responsabilité de gérer le risque ?
- Le conseil d'administration et le PDG fournissent-ils une autorisation claire au CRO pour aider les divisions ?
- Le CRO a-t-il une ligne hiérarchique directe avec le comité d'audit ou comité des risques ?
- Le PDG peut-il mettre fin à l'emploi du CRO ou d'autres cadres supérieurs, ou sont-ils indépendants de l'équipe de direction ?

- La fonction de gestion des risques dispose-t-elle d'un niveau approprié d'autorité, d'influence et d'indépendance au sein de l'organisation ?
- La fonction de gestion des risques dispose-t-elle de ressources et de compétences adéquates pour assumer son rôle ?
- Existe-t-il une seule personne ou une seule équipe chargée de coordonner les risques au sein de l'organisation ?
- L'approche de gestion des risques prend-elle en compte les scénarios de risque et l'interaction des risques multiples ?
- Quelle était la date de la dernière revue opérationnelle de la fonction de gestion des risques par l'audit interne et quel a été le résultat et les mesures prises par la direction ?

[11] Rapport final, Commission royale d'enquête sur les fautes professionnelles dans le secteur bancaire, des régimes de retraite et des services financiers, Commissaire Kenneth Hayne, 2019, Volume 1, p. 396.

Audit interne et audit externe

Le conseil d'administration doit s'assurer que le cadre de gestion des risques fonctionne efficacement et comme prévu.
L'efficacité peut être testée de temps à autre par des prestataires d'assurance tels qu'un audit interne ou externe.

Une entité cotée doit indiquer si elle dispose d'une fonction d'audit interne, comment cette fonction est structurée et quel rôle elle joue. Si elle n'a pas de fonction d'audit interne, elle doit divulguer les processus qu'elle utilise pour évaluer et améliorer l'efficacité de ses processus de gouvernance, de gestion des risques et de contrôle interne.12

Une fonction d'audit interne apporte une approche systématique et disciplinée pour évaluer et améliorer en permanence l'efficacité des processus de gestion des risques et de contrôle interne d'une organisation. Une fonction interne a un rôle unique dans la mesure où elle est basée au sein de l'organisation, mais est également indépendante et objective. Sa connaissance des pratiques au sein d'une organisation signifie également qu'elle est bien placée pour fournir une perspective sur les pratiques organisationnelles et la culture du risque en se basant sur ses observations des pratiques et des comportements.

Le responsable de la fonction d'audit interne doit avoir un lien hiérarchique direct avec le conseil d'administration ou avec le comité d'audit du conseil d'administration, et avec le ou les comités des risques s'ils sont distincts, afin de garantir l'indépendance de l'assurance.

Les petites organisations ne disposent peut-être pas d'une fonction d'audit interne, mais doivent être en mesure de démontrer les processus en place pour évaluer et améliorer en permanence l'efficacité de leurs processus de gestion des risques et de contrôle interne. Les petites organisations font souvent appel à un consultant externe pour fournir des services d'audit interne indépendants. Le conseil d'administration peut voir des avantages à faire appel à des consultants externes pour soutenir la fonction d'audit interne, ou à externaliser la fonction d'audit interne.

Les « trois lignes de défense » peuvent être un moyen utile de définir les rôles et les responsabilités lors de l'examen d'une gestion et d'un contrôle efficaces des risques :

- Première ligne — contrôle de gestion opérationnelle
- Deuxième ligne — assurance de gestion (fonctions de contrôle des risques et de surveillance de la conformité établies par la direction), et
- Troisième ligne — assurance indépendante.

Le conseil d'administration et ses comités ne sont pas inclus dans les « trois lignes de défense" mais sont servis par les "trois lignes". Son rôle est de veiller à ce que le modèle des "trois lignes de défense" soit reflétée dans la gestion et le contrôle des risques de l'organisation processus.

Il est important qu'il y ait une bonne compréhension des trois lignes de défense dans toute l'organisation.13 14

Les conseils d'administration doivent également être conscients que les régulateurs ont, ces dernières années, renforcé leur attention sur la qualité de l'audit.

Responsables hiérarchiques et employés de première ligne

Il peut être difficile de faire en sorte que la gestion des risques soit « vivante » pour tous les employés d'une organisation. Cela peut paraître ésotérique ou quelque chose qui ne concerne que la haute direction. Pourtant, la gestion des risques est l'affaire de tous et consiste à prendre des décisions commerciales éclairées en faisant prendre conscience des risques.

Dans la plupart des grandes organisations, une personne ou une équipe est responsable de la conception, de la mise en œuvre et du suivi du respect du cadre de gestion des risques. Elle peut également servir de « point de référence unique » en matière de gestion des risques et des menaces. L'ancienneté du responsable de la gestion des risques varie. Cependant, il est rare qu'une seule personne ou équipe soit chargée de coordonner les informations sur les risques dans l'ensemble de l'organisation et de synthétiser ces informations pour le conseil d'administration. En général, différentes équipes, par exemple celles des finances, des opérations, des relations publiques et de la direction, gèrent différents aspects des risques.

Les responsables d'entreprise gèrent quotidiennement les risques liés aux produits et services qu'ils proposent ou souhaitent proposer, mais ils peuvent avoir une compréhension limitée de la manière dont ces risques s'alignent ou s'écartent de l'appétence au risque ou de la stratégie de l'organisation. À l'inverse, les responsables qui soutiennent les unités commerciales, telles que les services juridiques, fiscaux et des ressources humaines, peuvent ne pas comprendre comment leur expertise s'applique spécifiquement aux produits et services de l'organisation.

Les lignes directrices du Governance Institute : la gouvernance à l'échelle de l'organisation fournissent un cadre permettant à une organisation de :

- veiller à ce que les efforts entrepris par tous les employés à travers l'organisation est alignée sur les objectifs stratégiques
- clarifier les rôles, les autorités et les responsabilités des individus dans la réalisation des objectifs stratégiques
- permettre aux individus de prendre des décisions alignées sur les objectifs stratégiques
- clarifier les contrôles et les limites qui s'appliquent à l'exercice de l'autorité, et
- prévoir une responsabilisation claire et efficace pour la décisions prises et autorité exercée.

Un cadre de gouvernance clair à l'échelle de l'organisation soutient la réalisation des objectifs stratégiques de l'organisation en précisant que la prise de décision est liée au risque et qu'il existe une responsabilité pour l'exercice de l'autorité.
Un tel cadre permet à tous les employés de s'adapter aux circonstances changeantes, tout en garantissant que les décisions sont prises dans le cadre de l'appétence au risque définie par le conseil d'administration.

[12] Voir la recommandation 7.3 Principes et recommandations en matière de gouvernance d'entreprise.

[13] Voir par exemple le rapport « Gouvernance du conseil d'administration sur les obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme chez Westpac : examen du comité consultatif », 8 mai 2020 à la page 14.

[14] Voir également le modèle des trois lignes de défense de l'IAA, Juillet 2020.

Questions aux réalisateurs :

- Existe-t-il des processus en place pour intégrer la gestion des risques dans la planification stratégique ?
- Le processus global de planification stratégique prendre en compte et hiérarchiser l'incertitude liée à la réalisation des objectifs stratégiques dans l'ensemble de l'organisation ?

- La direction doit-elle être encouragée à intégrer la création de valeur ainsi que la préservation dans son cadre de gestion des risques ?
- Le conseil d'administration évalue-t-il consciemment les risques et les récompenses lorsqu'il envisage des initiatives stratégiques majeures ?
- Le conseil d'administration évalue-t-il les plans stratégiques en fonction de leur échec potentiel et des conséquences qui en découlent ?

- Le conseil d'administration dispose-t-il d'un cadre adéquat pour comprendre les interrelations, les interdépendances et l'effet aggravant des risques ?
- Le conseil analyse-t-il les moyens proposés pour atteindre ces objectifs, ainsi que les contraintes probables ?
- Le conseil d'administration agit-il comme un catalyseur pour combler les cloisonnements au sein de l'entreprise en réunissant différents propriétaires de risques dans la même salle pour présenter leurs points de vue et leurs stratégies en matière de risques ?
- Le conseil a-t-il une opinion sur qui est le responsable désigné ? personne responsable de la gestion des risques au sein de l'organisation, la personne qui travaillera avec les propriétaires des risques, chacun d'entre eux étant responsable de la gestion opérationnelle de différents aspects du risque ? Il peut s'agir par exemple d'un CRO dans une organisation plus grande. ou le directeur financier ou le secrétaire d'entreprise dans une petite organisation.
- Le conseil d'administration est-il convaincu qu'il existe une communication et la compréhension entre les personnes chargées d'examiner la gestion des opportunités et les risques qui y sont associés à travers le

organisation et ceux qui sont responsables de l'articulation des messages organisationnels ?
- Le conseil d'administration répartit-il les risques de manière appropriée ? ressources de gestion ?

Risques ESG

Les actionnaires et les autres parties prenantes exercent une pression croissante pour que les entreprises prennent des mesures et publient des informations sur les questions ESG. Ces mesures impliquent souvent un volet de gestion des risques, notamment des demandes de divulgation des risques liés au changement climatique, de véritables engagements pour atteindre les objectifs de zéro émission nette et de désinvestissement des actifs liés aux combustibles fossiles.

Les risques sociaux à prendre en compte comprennent l'intimidation sur le lieu de travail, le harcèlement et les agressions sexuelles, les risques géopolitiques, les risques démographiques liés au vieillissement de la population australienne, les problèmes affectant les minorités culturelles et les risques éthiques tels que la corruption et l'esclavage humain dans les chaînes d'approvisionnement mondiales et nationales.

La gouvernance concerne la gouvernance des organisations et de nombreux investisseurs se concentrent sur les questions de gouvernance car ils considèrent que cela a un impact sur la valeur de leur investissement.

Risques liés au changement climatique

Le changement climatique pose des défis importants à l'Australie, affectant sa société, son économie et son environnement naturel.
L'Australie est particulièrement vulnérable à la sécheresse et aux feux de brousse, qui pourraient être exacerbés par le changement climatique.
Historiquement, le pays a largement dépendu des combustibles fossiles pour sa sécurité énergétique et sa croissance économique. Le changement climatique pose également des défis pour la biodiversité. Les investisseurs et autres parties prenantes, comme les régulateurs, demandent de plus en plus aux organisations de divulguer leur exposition au risque lié au changement climatique et sa gestion de celui-ci. Les autorités réglementaires accordent également une attention croissante au risque lié au changement climatique. Rien qu'en 2021 :

- L'ASIC s'est engagée à cibler les déclarations ESG trompeuses liées aux produits financiers dans le cadre de son plan d'entreprise 2021-2025 et a mis en garde contre des mesures réglementaires contre les déclarations trompeuses de zéro émission nette.15
- L'APRA a commencé son évaluation de la vulnérabilité climatique sur les cinq plus grandes banques australiennes pour aider à évaluer la vulnérabilité des institutions et la manière dont elles peuvent ajuster leurs modèles commerciaux en réponse au changement climatique.

En 2021, Noel Hutley SC et Sebastian Hartford-Davies ont mis à jour leur avis de 2016 sur le changement climatique. Dans leur avis de 2016, ils ont exprimé l'avis que le devoir de prudence et de diligence des administrateurs en vertu de la loi sur les sociétés permet ou oblige les administrateurs de sociétés australiennes à réagir aux risques liés au changement climatique. Selon eux, les administrateurs qui ne prennent pas en compte les risques liés au changement climatique pourraient être tenus responsables de manquement à leur devoir de prudence à l'avenir.

En 2021, ils affirment qu'il est « clair que les critères de référence des administrateurs en matière de changement climatique et des risques et opportunités qui en découlent continuent d'augmenter ».16

[15] Voir le discours, les priorités de l'ASIC en matière de gouvernance d'entreprise et l'année à venir, Joe Longo, président de l'ASIC, le 3 mars 2022.

[16] Voir Changements climatiques et devoirs des administrateurs, Mémoire d'opinion complémentaire, Noel Hutley SC et Sebastian Hartford-Davies, 23 avril 2021.

Ces dernières années, de nombreuses organisations ont annoncé des objectifs de zéro émission nette. Depuis la Conférence des Nations Unies sur les changements climatiques (COP 26), ce nombre est susceptible d'augmenter.17

Le risque lié au changement climatique aura un impact sur les organisations de tous les secteurs, soit en raison de leurs propres opérations, soit parce qu'il affecte leurs fournisseurs, leurs clients et d'autres parties prenantes. Pour ces raisons, les administrateurs doivent tenir compte de l'impact du changement climatique sur leur organisation et envisager des divulgations appropriées. Le Groupe de travail sur la divulgation financière liée au climat Le cadre TCFD (International Sustainability Standards Board) émerge rapidement comme le cadre privilégié pour la divulgation des risques matériels liés au climat.18 En 2022, l'International Sustainability Standards Board a été créé pour développer des rapports comparables par les entreprises sur le climat et d'autres questions ESG.

On constate également une augmentation significative des litiges liés au changement climatique. À l'échelle mondiale, le nombre cumulé de cas liés au changement climatique a plus que doublé depuis 201519. Cela représente un risque croissant pour les organisations de tous les secteurs.

Perte de la nature

Les risques financiers que représentent les pertes de nature pour les organisations font également l'objet d'une attention croissante. Le Groupe de travail sur la divulgation financière liée à la nature (TNFD) est une initiative mondiale, dirigée par le marché, dont la mission est de développer et de fournir un cadre de gestion des risques et de divulgation permettant aux organisations de signaler et d'agir sur l'évolution des risques liés à la nature. Le cadre TNFD s'appuie sur le cadre TCFD recommandations avec des informations à fournir dans quatre domaines : la gouvernance, la stratégie, la gestion des risques et les indicateurs et objectifs. Les recommandations finales du TNFD devraient être publiées en 2023.

Risques sociaux

Les investisseurs et autres parties prenantes s'intéressent de plus en plus à la manière dont les organisations gèrent un groupe de risques qualifiés de « risques sociaux » : les risques négatifs potentiels pour les organisations résultant de leurs impacts sur les communautés de personnes telles que les employés, les clients et les communautés locales. Un certain nombre d'échecs bien documentés

La gestion de ces risques a entraîné des dommages considérables, notamment en termes de réputation, pour un certain nombre d'organisations des secteurs public et privé.

Les risques sociaux comprennent :

- Esclavage moderne – cela inclut l'exploitation grave comme la traite des êtres humains, l'esclavage, la servitude, le mariage forcé, le travail forcé, la servitude pour dettes, les pires formes de travail des enfants et le recrutement trompeur pour le travail ou les services.20 Il est important pour les organisations d'identifier les risques d'esclavage moderne et de traiter de manière proactive les risques identifiés, y compris les risques dans leurs chaînes d'approvisionnement.

- Droits de l'homme – cela concerne les droits de l'homme des personnes sur lesquelles les organisations ont un impact, notamment au sein de leurs effectifs, de leurs communautés, de leurs clients et de leurs utilisateurs finaux. Les mauvaises pratiques peuvent exposer les organisations à des risques importants en termes de réputation et de finances.

- Faibles normes de travail – il y a eu un certain nombre de des scandales très médiatisés liés à la sous-rémunération du personnel. Les risques liés aux emplois précaires et précaires et aux conditions de travail dangereuses augmentent également.

- Sécurité au travail – La sécurité des employés ne concerne pas seulement la sécurité physique, mais aussi la santé mentale, et les organisations doivent veiller à ce qu'un soutien adéquat soit apporté au bien-être psychosocial des employés. Veiller à ce que les lieux de travail soient exempts de harcèlement sexuel est un élément de plus en plus fondamental pour assurer un environnement de travail sûr à tous les employés. La sécurité s'étend également à la prévention proactive et à la réponse efficace au racisme et aux autres formes de discrimination

- Diversité – Les organisations ont plus de chances de réussir lorsqu'elles exploitent l'intelligence collective et abordent les problèmes avec une diversité cognitive. Les organisations peuvent prendre en compte plusieurs aspects de la diversité, notamment le sexe, l'âge, l'éducation, l'expérience professionnelle et l'origine ethnique.

  Depuis quelques années, l'accent est également mis sur l'augmentation de la diversité des sexes au sein des conseils d'administration et des équipes de direction, en particulier dans les sociétés cotées.

[17] Voir Un guide pour le conseil d'administration et la direction sur la voie vers le zéro net, Institut de gouvernance d'Australie, 2022.

[18] Voir Divulgation des risques liés au changement climatique : Guide pratique pour rendre compte des principes et recommandations de gouvernance d'entreprise, Institut de gouvernance d'Australie, 2020.

[19] Voir Setzer, J., Higham, C., Les litiges liés au changement climatique se multiplient et ciblent les entreprises de différents secteurs, 2021.

[20] Voir la section 3 de la loi de 2018 sur l'esclavage moderne (Commonwealth).

Risques de gouvernance

Les risques de gouvernance sont liés aux risques découlant de mauvaises pratiques de gouvernance. Une bonne gouvernance est importante pour les actionnaires, les parties prenantes, les employés et les clients et est étroitement liée à la réputation d'une organisation.
Les mauvaises pratiques de gouvernance constituent donc une source de risques pour les organisations.

Le Governance Institute considère que la gouvernance comporte quatre éléments clés :

- Transparence – divulgation claire des informations sur la structure, le fonctionnement et la performance de l'organisation, tant en externe qu'en interne, et en maintenant un véritable dialogue avec les parties prenantes légitimes et le marché en général, et en leur fournissant des informations.
- Responsabilité – garantir la clarté de la prise de décision au sein de l'organisation, avec des processus en place pour garantir que les bonnes personnes disposent de l'autorité nécessaire pour que l'organisation prenne des décisions efficaces et efficientes, avec des conséquences appropriées en cas de non-respect de ces décisions processus.
- Intendance – développer et maintenir une reconnaissance à l'échelle de l'entreprise selon laquelle l'organisation est gérée au profit de ses actionnaires/membres, en tenant raisonnablement compte des intérêts des autres parties prenantes légitimes.
- Intégrité – développer et maintenir une culture engagée envers un comportement éthique et le respect de la loi.21

La reconnaissance et la gestion des risques constituent un élément essentiel du rôle du conseil d'administration, et la gestion et la supervision de la gestion des risques relèvent de sa responsabilité. La gestion des risques est un élément important de la gouvernance.

En Australie, la principale référence et le principal recours en matière de gouvernance d'entreprise reposent sur les dispositions de la loi sur les sociétés de 2001 et sur les principes et recommandations en matière de gouvernance d'entreprise.

Une bonne gouvernance garantit donc la transparence et la responsabilité et peut prévenir les scandales, les fraudes et les problèmes liés à la responsabilité organisationnelle. Une organisation qui fonde sa structure et sa culture d'entreprise sur des principes de bonne gouvernance a plus de chances d'éviter des catastrophes majeures.

Risques technologiques

Si les unités commerciales et les fournisseurs de services technologiques d'une organisation doivent disposer d'un registre des risques actif et d'une approche et d'une culture de gestion des risques, les risques technologiques peuvent également avoir un impact significatif sur les performances globales de l'organisation, l'expérience client et la réputation. Il est donc conseillé aux organisations d'établir un processus et des critères permettant d'inclure ou de faire remonter les risques technologiques ayant un impact stratégique ou opérationnel général aux niveaux de gouvernance et de gestion globale des risques appropriés au sein d'une organisation.

Risque cybernétique

Compte tenu de l'augmentation de l'activité en ligne au cours de la récente pandémie, combinée à une escalade significative des conflits mondiaux, le nombre de cyberattaques a augmenté de façon spectaculaire. Par conséquent, les organisations et leurs conseils d'administration accordent une attention accrue à ce risque. Dans le même temps, cette augmentation de l'activité en ligne à l'échelle mondiale a également été une source d'opportunités pour de nombreuses organisations, en leur ouvrant de nouveaux produits et marchés et en augmentant leur capacité à se connecter à leurs parties prenantes.

De nombreuses organisations utilisent le modèle de maturité des huit éléments essentiels du Centre australien de cybersécurité comme première étape vers l'amélioration de leur profil de risque en matière de cybersécurité.22

Une décision récente de la Cour fédérale a conclu qu'une société détenant une licence australienne de services financiers était en violation des dispositions de la Loi sur les sociétés en raison d'une conduite impliquant la cybersécurité.23 Il s'agit du premier cas dans lequel l'ASIC a exercé ses pouvoirs pour le manquement d'une organisation à disposer de contrôles adéquats de gestion des risques de cybersécurité et de cyber-résilience. Bien que cette affaire concerne une société de services financiers réglementée par l'ASIC, elle est également pertinente pour d'autres organisations qui peuvent faire l'objet d'un examen minutieux par d'autres régulateurs parce qu'elles sont soumises à des obligations similaires.24 Elles doivent s'assurer qu'il existe une surveillance rigoureuse des incidents afin d'identifier de manière proactive les problèmes systémiques plus larges ou les déficiences du système et qu'il n'y a pas de retard dans l'élaboration et la mise en œuvre de mesures de conformité améliorées une fois qu'une déficience a été identifiée.

Les conseils de bonnes pratiques de l'ASIC destinés aux sociétés de services financiers qui encouragent les activités visant à promouvoir la cyber-résilience constituent également un point de départ utile pour les organisations d'autres secteurs. L'ASIC considère que « la surveillance éclairée des risques implique que le conseil d'administration soit convaincu que les cyber-risques sont correctement traités par le cadre de gestion des risques de l'organisation. Les contrôles importants consistent notamment à s'assurer que l'organisation dispose de mesures de protection appropriées contre les activités cybernétiques malveillantes et que les capacités de récupération sont adéquates ».25 Les questions de l'ASIC ci-dessous constituent un guide utile pour les conseils d'administration lorsqu'ils envisagent la gestion des cyber-risques.

[21] Voir les fondements de la gouvernance sur www.governanceinstitute.com.au.

[22] Voir les sujets d' actualité Cyber-risque, Le Conseil des assurances d'Australie.

[23] Voir ASIC contre RI Advice Group Pty Ltd [2022] CAF 496.

[24] Voir également Ce que signifie une décision de la Cour fédérale sur la cybersécurité pour les titulaires de licence AFS, ASIC 2022.

[25] Voir les questions clés pour le conseil d'administration d'une organisation, sur www.asic.gov.au.

Questions aux administrateurs sur le cyber-risque

Cadre de gestion des risques

- Les cyber-risques font-ils partie intégrante du cadre de gestion des risques de l'organisation ?
- À quelle fréquence le programme de cyber-résilience est-il examiné au niveau du conseil d'administration ?
- Quel est le risque posé par les cybermenaces pour l'organisation ? entreprise?
- Le conseil d'administration a-t-il besoin d'une expertise supplémentaire pour comprendre le risque ?

Suivi des cyber-risques

- Comment surveiller le risque cybernétique et quelle escalade peut-il entraîner ? des déclencheurs devraient-ils être adoptés ?

Contrôles

- Quelle est la stratégie humaine en matière de cybersécurité ?
- Quelles mesures sont mises en place pour protéger les actifs d'information critiques ?

Réponse

- Que doit-il se passer en cas de violation ?

Les conseils d'administration devraient se poser les questions suivantes :

» Si et quand un problème survient, quels processus sont en place pour communiquer efficacement, en interne et en externe, et pour gérer la situation ?

» Le niveau de planification et de test des scénarios est-il suffisant pour garantir que les plans d'intervention sont valides et à jour, y compris avec les fournisseurs tiers et les personnes à charge ?26

À la suite d'une évaluation pilote par rapport aux exigences de la norme Prudential Standard CPS 234 Information Security, l'APRA a écrit à toutes les entités réglementées par l'APRA pour leur demander de renforcer leur capacité à superviser la cyber-résilience. Elle a indiqué qu'elle « s'attend à ce que les conseils d'administration aient le même niveau de confiance dans l'examen et la remise en question des questions de sécurité de l'information que lorsqu'ils gèrent d'autres questions commerciales ».27

Culture

Les concepts de culture du risque et de culture organisationnelle sont étroitement liés.

L'APRA considère, comme l'indique ce guide, que la culture du risque « n'est pas distincte de la culture organisationnelle, mais reflète l'influence de la culture organisationnelle sur la manière dont les risques sont gérés ».28 La culture d'une organisation est la somme de ses valeurs et comportements communs. Selon l'APRA, la culture organisationnelle inclut les valeurs et les comportements de ses collaborateurs en relation avec diverses dimensions, telles que le risque, mais ces dimensions ne sont pas des cultures distinctes.
On fait généralement référence à la culture d'innovation, à la culture de sécurité ou à la culture de conformité d'une organisation – celles-ci seraient, selon l'interprétation de l'APRA, simplement considérées comme des dimensions de la culture de l'organisation.
D'autres points de vue considèrent toutefois que la culture du risque d'une organisation est distincte de sa culture organisationnelle, et non pas un sous-ensemble de celle-ci. Prenons par exemple une organisation qui, dans l'ensemble, a une culture positive, mais qui présente des lacunes en matière de gestion des risques.

Compte tenu de cette diversité de points de vue, on peut affirmer avec certitude que la culture d'une organisation influence – positivement ou négativement – la manière dont elle gère et tolère le risque, et qu'à son tour, la culture du risque est capable de façonner la culture organisationnelle.

> « …la culture d'une entité peut être décrite comme « les valeurs et les normes partagées qui façonnent les comportements et les mentalités » au sein de l'entité. C'est ce que les gens font quand personne ne les regarde… »
> Commissaire Kenneth Hayne29

Il est également largement admis qu'un cadre de gestion des risques solide est bénéfique pour une culture d'entreprise saine car il favorise la responsabilisation. De même, l'immaturité des risques au sein d'une organisation peut ne pas permettre de limiter ou d'aggraver les principaux risques de conduite qui contribuent à des impacts négatifs sur la réalisation des objectifs de l'organisation et à des impacts préjudiciables sur les parties prenantes.

[26] Loc cit.

[27] Voir Insight Améliorer la cyber-résilience : le rôle que les conseils d'administration doivent jouer, APRA 23 novembre 2021.

[28] APRA, 2016, Document d'information : Culture du risque, p. 7.

[29] Commissaire Kenneth Hayne, Rapport final, Commission royale d'enquête sur les fautes professionnelles dans le secteur bancaire, des régimes de retraite et des services financiers (2019) Volume 1, p. 334.

Le rôle du conseil d'administration dans la culture

Le conseil d'administration est chargé de définir l'objectif d'une organisation et d'approuver sa déclaration de valeurs et son code. de conduite pour soutenir la culture organisationnelle souhaitée.

Un code de conduite reflète les valeurs fondamentales d'une L'organisation et les attentes des parties prenantes et de la communauté dans son ensemble doivent être prises en compte. Mais le simple fait d'avoir un code ne suffit pas : il faut également une formation régulière du personnel et une mise à jour occasionnelle du code.

Un élément clé de la culture est le comportement et la conduite des cadres supérieurs et du conseil d'administration lui-même. C'est ce que l'on appelle souvent le « ton donné par la direction ». Les normes éthiques et comportementales clairement définies de l'organisation doivent être renforcées dans la pratique par le groupe de direction de l'organisation. Le conseil d'administration et la direction doivent donner l'exemple et être perçus comme tels, car les employés suivront l'exemple des cadres supérieurs. Un certain nombre de scandales récents bien documentés concernant des conduites sexuelles inappropriées sur le lieu de travail soulignent l'importance du « ton donné par la direction ».30

La question pour les conseils d'administration est de savoir si la culture est connue et comprise et si la culture réelle (la culture vécue) représente la culture nécessaire et souhaitée.
un élément essentiel de la gouvernance qu'un conseil doit comprendre s'il existe un décalage entre la culture souhaitée et déclarée et la culture réelle, car c'est seulement la culture réelle – les valeurs promues – qui compte en fin de compte.

Une organisation peut avoir des sous-cultures, qui sont des groupes intra-organisationnels de personnes qui affichent un ensemble de valeurs et de comportements communs qui sont clairement différents de ceux des autres secteurs de l'organisation. Les conseils d'administration et la direction doivent identifier s'il existe des sous-cultures au sein de l'entité qui ne correspondent pas à la culture souhaitée de l'organisation dans son ensemble : toute sous-culture « rebelle » doit être identifiée.

Les règles sont nécessaires mais pas suffisantes pour inculquer une culture dans laquelle les valeurs promulguées correspondent aux valeurs souhaitées. De plus, sans une culture ouverte et transparente, le questionnement qui permettra de vérifier si les valeurs promulguées correspondent aux valeurs souhaitées n'aura pas lieu. Ces deux éléments sont au cœur de la gouvernance et de la gestion des risques s'ils doivent créer et protéger de la valeur pour l'organisation.

> Le défi pour le conseil d'administration est d'aller au-delà du simple exercice de conformité aux cases à cocher pour développer une culture organisationnelle dans laquelle le risque est véritablement pris en compte et géré à tous les niveaux de l'organisation.

Culture de la conscience du risque

La culture du risque d'une organisation correspond aux attitudes (valeurs) et comportements partagés des individus concernant la gestion des menaces et des risques au sein d'une organisation. La culture de l'organisation sera un déterminant clé de sa capacité à réagir et à s'adapter aux changements de l'environnement dans lequel elle évolue.

Pour gérer efficacement les risques et tirer parti des opportunités créées par l'incertitude, une organisation a besoin d'une culture de prise de conscience des risques. Une culture de prise de conscience des risques est un sous-ensemble essentiel de la une culture organisationnelle plus large qui intègre la manière dont les directeurs, les gestionnaires et les employés pensent, communiquent et se comportent à l'égard de tous les aspects du risque.

Les organisations doivent être attentives aux différences interculturelles et à leurs implications. Les individus jouent un rôle crucial dans la définition et le maintien des attitudes culturelles. Par conséquent, se concentrer sur les aspects particuliers de l'identité des individus qui peuvent avoir un impact sur la culture peut être un moyen important de comprendre pourquoi une culture fonctionne comme elle le fait. Le rôle de l'identité culturelle nationale des individus est influent sur la culture organisationnelle. Les cultures nationales ont des valeurs différentes et, par conséquent, des comportements différents peuvent être anticipés en réponse à une situation commune. Les recherches ont mis en évidence des différences nationales dans la façon dont les individus ont tendance à gérer l'incertitude, et ces différences sont importantes pour comprendre les attitudes des individus face au risque.31

Incitations

Les incitations jouent un rôle puissant en influençant les valeurs et le comportement des individus et donc la culture. Les incitations peuvent avoir des conséquences inattendues. Les recherches ont montré que les individus chercheront à faire les choses qui sont récompensées, implicitement ou explicitement, de manière tangible ou intangible, souvent à l'exclusion des activités qui ne sont pas récompensées. Cela peut créer
Il existe cependant des cas de folie où les types de comportement récompensés sont ceux que l'organisation tente de décourager, alors que le comportement souhaité n'est pas du tout récompensé.32

[30] Voir par exemple, Définir la norme : Rapport sur l'examen indépendant des lieux de travail parlementaires du Commonwealth, Commission australienne des droits de l'homme, novembre 2021.

[31] La théorie des dimensions culturelles de Hofstede, telle qu'articulée dans Culture's Consequences et Cultures and Organizations: Software of the Mind, co-écrit avec Gert Jan Hofstede.

[32] Kerr, S, « La folie de récompenser A, tout en espérant B », Academy of Management Journal, décembre 1975 ; 18, 000004, p 769.

> Lorsque les systèmes de rémunération sont conçus ou mis en œuvre de manière à ce que les dirigeants soient récompensés par des primes importantes malgré leur mauvaise gestion des risques, ces systèmes de rémunération augmentent la probabilité que l'entité se conduise mal ou adopte une conduite inférieure aux attentes de la communauté. En revanche, lorsque les systèmes de rémunération sont conçus et mis en œuvre de manière à tenir compte de la manière dont les dirigeants ont géré les risques – y compris le risque de non-conformité, le risque de conduite et le risque réglementaire – ces systèmes de rémunération réduiront la probabilité que l'entité se conduise mal ou adopte une conduite inférieure aux normes et aux attentes de la communauté.33
>
> Commissaire Kenneth Hayne

Questions aux administrateurs sur les incitations :

- Espérons-nous une croissance durable et à long terme — mais récompenser les ventes trimestrielles ?
- Espérons-nous un travail d'équipe – mais récompensons-nous le travail individuel ? effort?
- Espérons-nous des lieux de travail plus sûrs, mais récompensons-nous productivité et réduction des coûts ?
- Espérons-nous de la franchise, mais récompensons-nous la diffusion de bonnes nouvelles et l'accord avec le patron et punissons- nous la diffusion de mauvaises nouvelles ou le désaccord avec le patron ?
- Les incitations explicites et implicites sont-elles alignées sur les valeurs déclarées de l'organisation ou sur le cadre d'atténuation pour éviter toute prise de risque excessive ?

- Est-ce que cela est surveillé en permanence ?
- Le conseil d'administration inclut-il la gestion des risques comme critère d'évaluation des dirigeants ?
- Les pratiques de rémunération actuelles sont-elles alignées ou en contradiction avec la tolérance/capacité de risque des organisations ?

- Quel est le montant du salaire en jeu ?
- La rémunération fixe constitue-t-elle la part la plus importante du comportement à court terme ?
- La construction des systèmes de rémunération et des objectifs est-elle pilotée par les actionnaires avec des objectifs de performance à court terme ?

- Les objectifs liés aux risques sont-ils intégrés dans la stratégie de l'entreprise ? structures de rémunération des dirigeants ?

Évaluation par le conseil d'administration de la culture vécue

Pour un conseil d'administration, il peut être très difficile de comprendre dans quelle mesure la culture reflète les valeurs qu'elle défend. Il est tout aussi difficile pour un conseil d'administration de mettre en place les stratégies nécessaires pour développer une telle culture.

Les conseils d'administration reçoivent de plus en plus de rapports de type « tableau de bord » de la part de la direction sur des indicateurs clés tels que :

- les points de vue des parties prenantes sur la culture de l'organisation
- enquêtes sur l'engagement des employés
- enquêtes auprès des clients et leur degré de satisfaction
- enquêtes sur le comportement des dirigeants
- statistiques sur la santé et la sécurité au travail
- des statistiques clés sur les ressources humaines, telles que la rotation du personnel taux et tendances des entretiens de sortie
- des données de dénonciation anonymisées, et
- taux d'achèvement de l'éducation et de la formation.

Les conseils d'administration devraient appliquer les informations tirées d'indicateurs clés pour identifier, traiter et prévenir les causes profondes et les facteurs de risque sous-jacents conduisant à des fautes et à d'autres problèmes culturels, plutôt que de se concentrer sur des incidents isolés.

S'appuyer sur l'historique de l'entreprise ne donne pas un aperçu complet de la culture en vigueur au sein de l'organisation, bien que cela puisse faire partie des informations dont dispose le conseil d'administration pour se faire une idée de la mesure dans laquelle la culture reflète la vision du conseil.

Un conseil d'administration peut demander à des consultants externes de fournir un briefing aux administrateurs afin de les informer de ce qui s'est passé dans une entreprise qui n'a pas identifié ou géré ses risques, en leur fournissant une étude étape par étape du processus. Cela peut donner un aperçu des problèmes de culture qui n'auraient peut-être pas été mis en évidence à partir des résultats d'autres méthodologies utilisées.

33 Commissaire Kenneth Hayne, Rapport final, Commission royale d'enquête sur les fautes professionnelles dans le secteur bancaire, des régimes de retraite et des services financiers (2019) Volume 1, p. 347.

Questions à prendre en compte par les réalisateurs sur la culture :

- L'organisation dispose-t-elle d'une déclaration claire de Des valeurs ? Les employés doivent se sentir concernés pour s'investir véritablement dans de nouvelles valeurs. Dans les grandes organisations géographiquement diversifiées, veillez à trouver un équilibre entre la responsabilité locale et mondiale en matière de valeurs.
- Lors de la présentation d'un rapport sur la culture au conseil d'administration, devrait être un mélange d'indicateurs avancés et retardés et un travail interne sera nécessaire pour déterminer ce qui est approprié. Les indicateurs pourraient inclure : les plaintes des clients et des dénonciateurs, Rapports de violation, rapports réglementaires et enquêtes et la correspondance des régulateurs.
- Considérez comment les moteurs des mentalités culturelles, Les comportements et les résultats mentionnés dans le rapport de l'APRA (p. 82) opèrent dans l'organisation.
- Quelles sont les cultures dominantes dans votre organisation ? Où souhaite-t-elle se situer et comment y parvient-elle ?

- L'une de ces situations s'applique-t-elle à l'organisation :
  - » complaisance généralisée
  - » réactivité plutôt que préemption face au risque
  - » influence inégale de la fonction de risque
  - » ne met pas entièrement en pratique ce qu'il prêche en matière de gestion des risques
  - » Moins de tendance à la réflexion, à l'introspection et à l'apprentissage (à partir des erreurs)
  - » un environnement collégial et de grande confiance, conduisant à un excès de confiance et à une collaboration excessive
  - » s'efforçant d'équilibrer l'autonomisation et le défi, bien que pas bien exécuté
  - » vise à être une institution axée sur les valeurs, mais s'appuie trop sur les bonnes intentions
  - » une focalisation auto-perçue, mais incomplète, sur le client.

- Comment le conseil s'assure-t-il que les informations ne sont pas filtré par la haute direction ?
- La culture est-elle alignée avec la stratégie de l'organisation ?
- Comment fonctionne le cadre de responsabilisation dans l'organisation?
- Le cadre de gestion du rendement aborde-t-il le « comment » et pas seulement le « quoi » ?
- La direction peut-elle fournir rapidement et facilement au conseil d'administration et à la haute direction des informations appropriées sur les performances et les récompenses ?
- La haute direction modélise-t-elle la performance de l'organisation ? Des valeurs ? Comment le démontrent-ils ?

Outils, processus et améliorations

La section suivante présente les outils, processus et améliorations courants qui peuvent aider les administrateurs à déterminer comment ajouter de la valeur à leur conseil d'administration dans le domaine de la gestion des risques et à garantir que leur organisation gère efficacement les risques. Les administrateurs devront décider si ces outils sont adaptés à leur situation personnelle.

Meilleure intégration du risque et de la stratégie

La gestion des risques et la stratégie sont les deux faces d'une même médaille et doivent être régulièrement liées dans les discussions du conseil d'administration et des comités du conseil.

La gestion des risques devrait être explicitement intégrée au processus de planification stratégique.

Le conseil d'administration doit tenir la direction responsable de l'élaboration et de l'exécution d'une stratégie qui correspond à l'appétence au risque qu'il a définie.

Question clé pour les réalisateurs :

- Les ordres du jour du conseil d'administration favorisent-ils l'intégration des questions de risque avec d'autres points de l'ordre du jour tels que la stratégie, la structure organisationnelle et les finances ?

Une taxonomie partagée du risque

Les organisations ont intérêt à utiliser une taxonomie commune des risques comme base du cadre de contrôle des risques, afin de garantir qu'une vision unifiée des risques soit partagée par le conseil d'administration, la haute direction et toutes les unités commerciales. Un langage commun des risques permet d'unifier les différentes disciplines dans l'effort conjoint visant à atteindre les objectifs organisationnels.

Une taxonomie complète permet de trier les risques en niveaux de hiérarchie, y compris les principales catégories de risques, les sous-catégories de risques et les types de risques qui prennent en charge d'autres parties critiques de la gestion des risques, notamment l'identification des risques, l'atténuation des risques et, en fin de compte, les rapports du conseil d'administration.

Il existe de nombreuses taxonomies qui peuvent être adaptées au secteur et à l'environnement opérationnel de l'organisation. Une taxonomie dans un contexte clinique tel que celui des maisons de retraite peut différer sensiblement de celle des services financiers, par exemple.

Un exemple de taxonomie est 52 Risks®.

Un défi potentiel consiste à parvenir à une définition et à une taxonomie convenues des risques non financiers, car ceux-ci sont souvent définis par l'exclusion des risques financiers.

Appétence au risque et tolérance au risque

Au niveau le plus large, le plan stratégique/d'affaires est l'expression par le conseil d'administration de l'appétence au risque d'une organisation.
Cependant, il est de plus en plus courant que les conseils d'administration publient une déclaration formelle d'appétence au risque distincte de leur stratégie.

Les entités réglementées par l'APRA sont tenues de disposer de déclarations d'appétence au risque approuvées par le conseil d'administration, et il est de bonne gouvernance pour les conseils d'administration des sociétés cotées d'établir l'appétence au risque – voir les Principes et recommandations de gouvernance d'entreprise.34

La définition de l'appétence au risque exprime explicitement les attitudes et les limites du risque que le conseil d'administration attend de la direction générale et dans lesquelles il s'attend à ce que la direction agisse pour atteindre les objectifs stratégiques de l'organisation. Une appétence au risque réfléchie et clairement formulée constitue une base solide pour la gestion des risques.

Différence entre l'appétence au risque et la tolérance au risque ?

Le guide COSO, Enterprise Risk Management — Integrating with Strategy and Performance, définit l'appétence au risque comme suit : les types et le niveau de risque, à un niveau général, qu'une organisation est prête à accepter dans la recherche de valeur.35 L'appétence au risque est stratégique et fait référence à l'approche globale de l'organisation face au risque. La tolérance au risque est l'application pratique de l'appétence au risque à des transactions ou activités spécifiques.

Les plans stratégiques de l'organisation sont liés à l'appétence au risque, tandis que les plans d'affaires au niveau de l'unité commerciale sont liés à la tolérance au risque. Les deux concepts sont parfois utilisés de manière interchangeable. Néanmoins, ils peuvent être mentionnés conjointement dans une déclaration d'appétence au risque approuvée par le conseil d'administration. Par exemple, la politique de gestion des risques du Commonwealth du ministère des Finances (RMG 211) encourage les entités à élaborer une « déclaration d'appétence et de tolérance au risque ». La déclaration approuvée par le conseil d'administration peut être constituée d'énoncés d'appétence au risque de haut niveau en un ou deux paragraphes seulement, qui à leur tour conduisent à une liste plus détaillée des tolérances au risque. Dans cet exemple, les deux parties fonctionnent ensemble et constituent ensemble la déclaration d'appétence au risque.

Sans une compréhension commune de l'appétence au risque et un alignement entre le conseil d'administration et la direction, la gestion des risques peut être effectuée avec des attentes floues.
Cela peut aboutir à une culture où les décisions sont prises sans tenir compte des risques et sont incompatibles avec les appétence au risque souhaitée.

L'appétence au risque doit être exprimée de manière significative et l'appétence au risque déclarée par le conseil d'administration doit correspondre à l'appétence au risque en vigueur au sein de l'organisation.
L'appétence au risque d'une organisation peut varier au fil du temps, en cas de crise, dans différentes régions géographiques, pour différentes unités commerciales ou pour différentes catégories de risques. La déclaration doit être suffisamment descriptive pour permettre à son public de comprendre l'approche adoptée par l'organisation pour gérer le risque et la pondération du risque par rapport à la récompense potentielle. Elle peut être à la fois quantitative et qualitative.

Bien que les régulateurs puissent prescrire une gamme de contenus pour la déclaration, il est généralement admis qu'une telle déclaration doit refléter :

- stratégie de l'organisation — objectifs, plans d'affaires, attentes des parties prenantes
- la capacité d'une organisation à absorber les pertes — la tolérance aux pertes ou aux événements négatifs qui peuvent être raisonnablement quantifiés
- la position éthique de l'organisation, les activités qui ne sont pas acceptables et les classes de risques à éviter
- les compétences, les ressources et la technologie nécessaires pour gérer et surveiller les expositions
- la volonté de l'organisation d'investir dans la poursuite de ses objectifs stratégiques — il peut exister plusieurs appétences au risque pour différents types ou sources de risque, et
- le retour sur investissement attendu — c'est-à-dire le montant que l'organisation est prête à dépenser pour améliorer les résultats probables.

Registres et matrices de risques

Les matrices de risques sont généralement adoptées par les conseils d'administration et affinées par la direction pour évaluer les risques au sein de l'entreprise. Les critères utilisés dans la matrice de risques doivent être adaptés au contexte de l'organisation et cohérents avec son appétence au risque.

Il existe une large gamme de modèles de matrices de risques conformes aux meilleures pratiques. Les conseils d'administration doivent s'appuyer sur ces modèles, mais s'assurer qu'ils sont adaptés à l'organisation.

[34] Voir la norme APRA Prudential Standard CPS 220 Gestion des risques et les Principes et recommandations de gouvernance d'entreprise 1.1, 7.1 et 7.2.
[35] Voir le Guide sur la gestion des risques d'entreprise Gestion des risques d'entreprise – Intégration à la stratégie et à la performance 2017.

Analyse de données, approches quantitatives et tableaux de bord

La plupart des organisations ont la possibilité d'améliorer la nature et le type d'indicateurs de risque clés inclus dans les systèmes de reporting et de tableau de bord du conseil d'administration. Une enquête menée en 2020 par le Governance Institute auprès de professionnels de la gouvernance et des risques et de cadres supérieurs a révélé que, lorsqu'on les interrogeait sur le reporting des risques de leur organisation au conseil d'administration, près de la moitié (49 %) déclaraient qu'il n'était que « assez efficace » et près d'un quart (21 %) le jugeaient « peu efficace ».36

Les systèmes sophistiqués de gestion des risques fournissent un ensemble de statistiques quantitatives qui peuvent constituer une riche source d'informations pour les conseils d'administration et la direction.

L'utilisation croissante de l'analyse des données peut également offrir au conseil d'administration l'occasion de demander à la direction de renforcer les tableaux de bord afin d'inclure davantage d'informations, notamment des indicateurs avancés et retardés, qui aident à suivre les risques.
Les indicateurs avancés servent de signaux d'alerte précoce concernant des problèmes potentiels et peuvent indiquer des réussites qui peuvent être davantage exploitées.

Lorsque les données sont utilisées pour éclairer la prise de décision du conseil d'administration, maintenir la qualité des données devient critique. Le conseil d'administration et la direction doit s'assurer qu'il existe des systèmes et des processus en place pour assurer l'exactitude, la cohérence, la sécurité et que les données les plus à jour parviennent au conseil.

Matrice des compétences du conseil d'administration

Le renouvellement du conseil d'administration est essentiel à la performance. Le conseil d'administration doit évaluer régulièrement la composition et l'efficacité du conseil dans son ensemble, ainsi que tout besoin futur de nouveaux administrateurs. Cela comprendra un examen de la combinaison requise de compétences, d'expérience et d'autres qualités des administrateurs. Une matrice de compétences est un outil utile pour aider le conseil d'administration pour déterminer la bonne combinaison de directeurs et comprendre ses besoins en compétences supplémentaires et identifier les éventuelles lacunes.
Une matrice de compétences est essentielle au processus de sélection des administrateurs. Elle fonctionne comme un outil de gestion des risques pour le conseil d'administration. Les facteurs à prendre en compte lors de l'élaboration d'une telle matrice peuvent inclure non seulement les compétences et l'expérience, mais aussi les qualités personnelles et la diversité requises des administrateurs, à la fois collectivement et individuellement.

Compétence en matière de risque des administrateurs

Les conseils d'administration, collectivement, et les administrateurs individuellement devraient s'assurer, par le biais d'évaluations périodiques, que les compétences des administrateurs sont appropriées pour superviser efficacement les risques.

Les lacunes dans les compétences ou les connaissances collectives nécessaires peuvent être comblées par l'éducation et la formation et par le processus de sélection des nouveaux administrateurs.

La formation des conseils d'administration dans le domaine de la gestion des risques peut bénéficier d'une approche structurée, en particulier lorsque les organisations opèrent dans des secteurs hautement techniques et dynamiques. Le conseil d'administration peut envisager de consacrer une partie de son budget de formation à la formation en gestion des risques.
Il peut également être approprié d'organiser un mentorat pour les nouveaux directeurs dans les domaines où l'organisation est confrontée à des risques émergents, comme la cybersécurité.

L'importance de la culture du conseil d'administration

La culture du conseil d'administration et la dynamique comportementale sont fondamentales pour le processus décisionnel de gestion des risques et de supervision de la stratégie.

Les décisions du conseil d'administration en matière de risque et de stratégie sont prises en groupe, ce qui présente de nombreux avantages, notamment l'accès à un plus grand bassin de connaissances et une plus grande acceptation de la décision finale du conseil. Cependant, une mauvaise dynamique de groupe peut également entraîner une réflexion étroite, la suppression des points de vue divergents, des jugements superficiels et une incapacité à découvrir les risques nouveaux et émergents et les faiblesses potentielles du cadre de gestion des risques.

Tous les administrateurs doivent contribuer à un dialogue ouvert, franc et dynamique sur les risques et la stratégie, remettre en question de manière constructive les hypothèses, faire preuve d'un niveau approprié de scepticisme et envisager explicitement des perspectives alternatives. Ils doivent équilibrer cela avec discrétion et respect mutuel.

En fin de compte, chaque administrateur doit soutenir la décision finale du conseil d'administration en matière de risque et de stratégie, qu'il y soit initialement favorable ou non.

[36] Rapport d'enquête sur la gestion des risques 2020, Institut de gouvernance d'Australie, p. 9.

Les informations circulent vers le conseil d'administration

Il est essentiel de fournir au conseil d'administration des informations fiables et opportunes sur les risques.

Les protocoles d'information au sein de l'organisation doivent permettre et anticiper l'évolution constante du paysage dans lequel les entreprises évoluent.

Le conseil d'administration doit reconnaître que le fait de ne pas agir sur la base des informations dont il dispose peut être tout aussi dommageable que de ne pas disposer de ces informations du tout.

La gestion des risques est souvent incluse dans les rapports du PDG au conseil d'administration. Cette approche présente l'avantage de permettre au conseil d'administration d'obtenir l'assurance du plus haut niveau de direction que les risques sont gérés de manière appropriée. Toutefois, les rapports du PDG sur les risques sont souvent préparés sans l'avis des employés de l'ensemble de l'organisation. Il se peut que les informations clés sur les risques ne parviennent pas au conseil d'administration. Les gestionnaires des risques et les employés de première ligne ayant accès aux informations clés sur les risques ne disposent pas toujours de l'ancienneté nécessaire pour garantir que ces informations sont transmises au niveau approprié.

Le conseil d'administration doit s'assurer que les informations sur les risques qui lui sont fournies sont complètes et fiables et que la direction met en œuvre tous les efforts raisonnables pour y remédier. Le conseil d'administration peut créer des lignes de communication supplémentaires sur les risques.
Les administrateurs individuels peuvent également chercher à découvrir l'organisation au niveau opérationnel et client par le biais de visites sur place, par exemple en passant la nuit dans des établissements tels que des résidences pour personnes âgées ou par d'autres moyens.

Une compréhension plus approfondie de l'organisation, de son modèle économique, de ses clients, de ses employés et de son impact sur les communautés dans lesquelles elle opère permettra aux administrateurs de gérer plus efficacement les risques et de jouer un rôle plus actif dans les discussions du conseil d'administration et dans l'engagement avec la direction.

Planification des incidents critiques et de la continuité des activités

La planification de la continuité des activités et des incidents critiques est devenue un élément de plus en plus important de la gestion des risques dans de nombreux secteurs. L'objectif est de minimiser l'impact d'une crise ou d'une urgence résultant d'incendies de forêt, d'inondations, de pandémies, d'actes terroristes, de violations majeures de la cybersécurité ou d'incidents connexes.

Dans le cadre de ce processus de planification, certaines organisations effectuent des évaluations annuelles des menaces et des scénarios fictifs et développent des installations de reprise d'activité autonomes pour permettre la continuité des activités. Les processus de planification peuvent ou non être menés dans le même domaine que la fonction de gestion des risques dédiée dans le cadre de la gestion des risques.

mesures d'atténuation. Une étude des pratiques de gouvernance au cours de la première phase de la pandémie de COVID-19 a révélé que « trop d'organisations ont été prises par surprise par la pandémie de COVID-19 parce qu'elles n'avaient pas de plan de continuité complet, les conseils d'administration et la direction préparant plutôt des « ateliers » d'urgence en temps réel ».37 Depuis la COVID-19, de nombreuses organisations accordent désormais une attention accrue à la planification des imprévus et des scénarios et testent des plans de crise et de continuité des activités.

Le conseil d'administration doit s'assurer que ces processus de planification sont intégrés au cadre de gestion des risques.

Fréquence des délibérations du conseil d'administration sur les risques

La gestion des risques doit être formellement incluse dans les rapports du conseil d'administration et inscrite à l'ordre du jour à une fréquence et une régularité compatibles avec l'appétence au risque de l'organisation afin que le conseil d'administration puisse s'assurer que le cadre de gestion des risques reste solide.

Le secrétaire de la société prépare généralement un agenda annuel qui énonce les points réguliers à examiner lors de réunions particulières du conseil d'administration et des comités tout au long de l'année, y compris les sujets relatifs à la gestion des risques, ainsi qu'un calendrier pour la soumission des documents et, par conséquent, la fourniture des documents du conseil au conseil. Les administrateurs doivent s'assurer que le temps alloué à la gestion des risques tout au long de l'année est suffisant et que le calendrier prévoit suffisamment de temps pour l'examen des documents du conseil par toutes les parties concernées et pour l'obtention des approbations de la direction. Chaque organisation aura ses propres étapes d'approbation obligatoires qui sont requises dans le cadre de ce processus.

Certains conseils d'administration choisissent d'inscrire la gestion des risques à l'ordre du jour afin de s'assurer qu'elle bénéficie d'une attention et d'une attention constantes. La pertinence ou non de cette démarche dépendra des circonstances propres à l'organisation, notamment de la fréquence des réunions du conseil d'administration et des comités.
Le défi avec un point permanent à l'ordre du jour est de veiller à ce qu'il ne devienne pas obsolète et routinier au fil du temps et ne conduise pas à une « homologation automatique » des recommandations de la direction.

Certaines organisations mènent leurs discussions sur les risques au moment de la publication des rapports annuels et à l'occasion de l'assemblée générale annuelle. Cela peut créer des problèmes de calendrier et de ressources, car les élections des administrateurs, la rémunération et d'autres questions requièrent l'attention du conseil d'administration. Le meilleur moment pour engager le conseil d'administration sur la gestion des risques peut être pendant les périodes moins chargées du calendrier financier.

Quelle que soit la manière dont le conseil d'administration choisit d'aborder la question, la gestion des risques doit faire l'objet d'un dialogue permanent afin d'encourager une amélioration continue. La documentation de gouvernance doit indiquer quels sujets de gestion des risques seront abordés lors de quelles réunions.

[37] Voir La gouvernance à travers la crise Apprendre de la COVID-19 Leçons pour aujourd'hui et pour l'avenir, Governance Institute of Australia et Australian Institute of Company Directors, 2020 à la page 28.

Documents et rapports du conseil d'administration

La communication des programmes et initiatives de gestion des risques est avant tout une aide à la bonne gouvernance. La communication des informations sur les risques doit avoir pour but d'éclairer la prise de décision du conseil d'administration. Ce type d'informations donne l'assurance que les processus et pratiques de gestion des risques sont efficaces, bien situés sur le plan fonctionnel, connectés et pertinents pour l'entreprise et qu'ils sont activement gérés et améliorés.

Les documents du conseil d'administration sont le principal moyen par lequel les administrateurs obtiennent les informations nécessaires pour remplir leur rôle de gestion des risques. Pour aider les administrateurs à s'acquitter de leurs fonctions, les informations contenues dans les documents du conseil doivent être cohérentes, complètes dans la mesure nécessaire et uniformes. Dans la Commission royale sur les services financiers, le juge Hayne a noté que les conseils d'administration doivent disposer des « bonnes informations pour s'acquitter de leurs fonctions »38. Ses commentaires réitèrent l'importance d'améliorer la qualité des informations (et non d'augmenter la quantité d'informations) fournies aux conseils d'administration afin que les administrateurs soient en mesure de s'acquitter efficacement de leurs fonctions.

Des documents de conseil bien rédigés et concis jouent un rôle important pour garantir que les administrateurs disposent des informations nécessaires pour contribuer aux discussions du conseil et permettent au secrétaire de la société de consigner succinctement les délibérations et les résolutions d'une réunion dans le procès-verbal. Un document de conseil bien rédigé identifiera la justification des résolutions proposées. Cela permet de concentrer les discussions du conseil sur les questions clés soulevées dans le document et sur toute information ou clarification supplémentaire requise par le conseil. Pour que les documents du conseil remplissent cette fonction importante, il faut apporter le soin approprié à leur préparation.

Il est essentiel que les administrateurs jouent un rôle actif en s'assurant que les documents du conseil sont adéquats et qu'ils disposent d'informations suffisantes et « correctes » sur lesquelles fonder leurs décisions et exercer leurs fonctions de surveillance et de contrôle. Cela comprend la contribution au document du conseil processus, en articulant leurs attentes quant à la qualité et à la suffisance des informations à fournir et en veillant à ce qu'il existe des systèmes et des processus de contrôle pour maintenir l'intégrité des informations.

En 2019, une étude de l'ASIC a révélé que, dans l'échantillon examiné, la taille des dossiers des comités des risques était en moyenne de 300 pages, les documents d'une organisation faisant en moyenne un peu plus de 700 pages. L'ASIC a recommandé de ne pas utiliser de dossiers de conseil « denses et volumineux ». Le régulateur a encouragé les organisations à « garantir des rapports de gestion concis ». « Nous ne pensons pas que l'imposition et l'application d'une limite maximale de pages résoudra ce problème. Mais le fait que les directives spécifiques à l'organisation ne soient pas appliquées suggère que les présidents ne se sont pas suffisamment intéressés à la nature des rapports qui leur sont fournis », a conclu l'ASIC.39

La préparation des documents du conseil d'administration incombe principalement à la direction, les secrétaires d'entreprise jouant également un rôle essentiel. Le secrétaire d'entreprise doit collaborer avec la direction pour produire des documents qui précisent clairement ce que le conseil d'administration ou le comité du conseil d'administration est chargé de faire. Pour plus d'informations sur les documents du conseil d'administration, consultez les conseils 2021 du Governance Institute sur les documents du conseil d'administration.

Aucun dossier commercial ne devrait être présenté au conseil d'administration sans une évaluation appropriée des risques jointe à la proposition. Le processus d'évaluation des risques, qui conduit à des conseils sur les options qui seront finalement prises en compte par le conseil d'administration, doit inclure des données quantitatives qui suivent la performance de la direction dans la mise en œuvre de la stratégie convenue par le conseil d'administration. Il devrait également inclure des données qualitatives, mais ne pas en dépendre uniquement.

Le comité des risques, le cas échéant, doit examiner et approuver les mesures et la méthodologie utilisées pour étalonner la performance par rapport à l'appétence au risque. Il est essentiel que la direction et le conseil d'administration aient une idée claire des leviers à actionner pour gérer tout risque identifié pour la valeur de l'organisation.

[38] Commissaire Kenneth Hayne, Rapport final, Commission royale d'enquête sur les fautes professionnelles dans le secteur bancaire, des régimes de retraite et des services financiers (2019) Volume 1, p. 400.

[39] ASIC (2019) Groupe de travail sur la gouvernance d'entreprise, rapport sur la surveillance des risques non financiers par les administrateurs et les dirigeants, pp. 27-28.

Questions aux administrateurs sur les rapports du conseil d'administration :

- L'étendue et la matérialité des informations qui la direction fournit-elle des informations correctement calibrées pour nous aider à remplir notre fonction de surveillance ?40
- Les informations que nous recevons sur les risques non financiers d'une qualité similaire à celle que nous recevons sur le risque financier ?41
- Les éléments de la gestion des risques sont-ils Le cadre fonctionne-t-il comme prévu et fournit-il les avantages recherchés ?

- À quelle fréquence le conseil d'administration discute-t-il des risques avec gestion?
- Comment la direction aborde-t-elle les principaux opportunités et risques auxquels l'organisation est confrontée ?
- Comment le conseil d'administration sait-il qu'il s'agit bien des principales opportunités et des principaux risques et que les mesures prises par la direction pour y faire face sont appropriées ?

- Quels sont les 5 à 10 principaux risques et stratégies d'atténuation surveillés ?
- Quels sont les risques susceptibles d'entraîner une anomalie significative dans les états financiers annuels ? déclarations ?
- Comment le conseil d'administration sait-il quand les risques sont en augmentation, en stabilité ou en diminution ?
- Comment le risque est-il intégré dans le plan d'affaires et l'élaboration de la stratégie ?
- La hiérarchie des risques est-elle toujours adaptée à son objectif ?
- Existe-t-il une analyse du point de vue des principaux des groupes de parties prenantes tels que les clients, le personnel, les investisseurs, les régulateurs, les communautés, qui pourraient révéler des domaines de risque pour la viabilité continue que les approches analytiques traditionnelles peuvent manquer ?
- Le conseil a-t-il l'assurance qu'il reçoit les informations dont elle a besoin ?
- Quel niveau d'assurance le conseil souhaite-t-il ?
- Des contrôles sont-ils en place pour enquêter sur la qualité des les informations qui circulent au conseil ?
- Toutes les propositions sont-elles présentées au conseil d'administration non seulement avec une analyse de rentabilisation, mais aussi avec une évaluation des risques et Le reporting sur les projets inclut-il le reporting des risques ?
- La même discipline appliquée au reporting habituel s'applique-t-elle aux décisions concernant les nouveaux projets ?

- La gestion des risques est-elle intégrée à tous les systèmes de l'entreprise, tels que la gestion des performances, la gestion des processus et la mise en œuvre de la stratégie ?

Engagement auprès des investisseurs sur les questions de risque

La gestion des risques est un sujet sur lequel il est de plus en plus intéressant pour les conseils d'administration de s'engager spécifiquement auprès des investisseurs et des membres, notamment auprès des actionnaires particuliers et institutionnels, sur les questions ESG.

Une communication active, informée, constructive et périodique entre le conseil d'administration et les actionnaires est essentielle pour une mutuelle.
compréhension de la stratégie d'entreprise, du risque et de la surveillance des risques.

Le dialogue doit être fondé sur une approche appropriée et réciproque.
niveau de respect, de confiance, d'ancienneté, de compétence et de professionnalisme.

Assurance

L'assurance est une forme de transfert de risque dans laquelle une autre entité assume un risque pour l'entité où réside le risque. Le transfert de risque est un élément important de la gestion des risques avec lequel les administrateurs doivent se familiariser.

Le conseil d'administration, en consultation avec la direction, doit déterminer le type de produits d'assurance et les niveaux de couverture appropriés pour les expositions aux risques présents et futurs de l'organisation. Le registre des risques et d'autres éléments importants du cadre de gestion des risques seront utiles dans le processus annuel de renouvellement des assurances.

Un domaine important à prendre en compte est l'assurance de cybersécurité. Ce type d'assurance concerne les cybermenaces et les cyber-risques et de nombreuses organisations souscrivent désormais des polices d'assurance cyber. Ces produits diffèrent d'un fournisseur à l'autre et d'une juridiction à l'autre, mais incluent généralement une couverture pour les enquêtes médico-légales, la restauration des données, la notification et la rectification des clients, par exemple pour les centres d'appels, et l'indemnisation des pénalités imposées par les régulateurs gouvernementaux. Depuis le début de la COVID-19, les coûts de cette assurance ont augmenté.
Les primes d'assurance ont augmenté de façon spectaculaire et « la combinaison d'un bassin de primes restreint et de la sophistication et de la malveillance croissantes de certaines cyberattaques a exercé une pression considérable sur les assureurs et les entreprises. »42

40 ASIC (2019) Groupe de travail sur la gouvernance d'entreprise, rapport sur la surveillance des risques non financiers par les administrateurs et les dirigeants, p. 28.

41 Ibid.

42 Voir le document de réflexion Cyberassurance : protéger notre mode de vie dans un monde numérique. L'ICA appelle à une refonte des paramètres de la politique cybernétique, Insurance Council of Australia, mars 2022.

Projets et gestion des risques

Les équipes de projet apportent souvent des compétences, des contacts et une expérience externes et donc une nouvelle perspective à une organisation. Étant donné que les projets sont de nature temporaire avec des budgets, une portée et des calendriers fixes, les membres de l'équipe se concentrent sur l'identification des risques qui peuvent avoir un impact sur la livraison du projet. Les équipes de projet travaillent également généralement avec différents niveaux d'une organisation, ce qui peut différer de la manière dont les risques sont gérés dans une organisation. Elles travaillent avec les organisations pour les aider à élaborer des analyses de rentabilisation et discutent fréquemment avec le personnel pour identifier de nouveaux risques organisationnels qui constituent potentiellement des avantages supplémentaires pouvant être inclus dans le plan de réalisation du projet. Elles ont également une conscience accrue des risques liés à la mise en œuvre des changements envisagés par le projet.

Les CRO et leurs équipes collaborent généralement de manière horizontale avec les dirigeants de l'organisation pour les aider à examiner, analyser et surveiller le traitement des risques organisationnels les plus élevés. Les dirigeants, à leur tour, travaillent généralement de manière verticale avec leurs divisions pour identifier, évaluer, gérer et surveiller les risques d'une division. Pour mener à bien un projet, l'équipe de projet devra travailler à la fois verticalement et horizontalement et peut fréquemment découvrir des risques qui n'étaient peut-être pas apparents. Les projets peuvent donc être un canal supplémentaire précieux pour identifier les risques internes, externes et émergents.

Risques non financiers et émergents

Événements à risque significatifs impliquant des risques non financiers, notamment La pandémie de COVID-19, l'attention mondiale portée au harcèlement sexuel au travail et la recrudescence des cyberattaques ont considérablement accru l'importance de ce domaine dans l'esprit des administrateurs, des régulateurs et des parties prenantes. Les conseils d'administration de tous les secteurs sont aux prises avec ce domaine en pleine expansion.

Selon le rapport sur les risques mondiaux (2022) du Forum économique mondial, Les 10 principaux risques auxquels les entreprises seront confrontées au cours de la prochaine décennie sont principalement d'ordre environnementaux, géopolitiques et sociétaux, et non financiers.

Le risque non financier est un concept large et fluide, généralement défini par exclusion. Certaines organisations préfèrent des termes tels que « pré-financier » ou « émergent » pour reconnaître ces risques qui ont souvent des impacts financiers. Cependant, la catégorie est généralement compris comme incluant les thèmes décrits ci-dessous.

Comme indiqué précédemment dans le guide, il est important pour les organisations d'élaborer une taxonomie commune des risques qui inclut une définition des risques non financiers.

> Le défi pour un conseil d'administration est d'adopter une approche plus proactive dans la gestion des risques non financiers.

En particulier, les attentes des communautés sur les questions environnementales et sociales sont de plus en plus élevées dans tous les secteurs.

L'essor des technologies numériques présente des opportunités, mais aussi des menaces et des défis éthiques. La pandémie de COVID-19 nous rappelle également l'importance de gérer les risques pour la santé publique et l'interdépendance de tous les secteurs dans un monde globalisé. économie.

Dans le cadre de leur évaluation des risques, les conseils d'administration devraient activement prendre en compte ces risques et d'autres risques non financiers importants et émergents.

Réputation

Les risques de réputation découlent souvent d'autres catégories de risques. Les atteintes à la réputation sont souvent causées par une défaillance de la gestion des risques dans d'autres domaines. Il est de plus en plus admis que les modèles économiques reposent sur la confiance dans l'organisation.

Les risques de réputation peuvent survenir lorsque la réputation d'une organisation est entachée en raison d'un décalage entre les perceptions du public et les objectifs et ressources réels de l'organisation. Une faute grave, une défaillance humaine ou des systèmes, une conduite contraire à l'éthique, une panne majeure du système informatique, une atteinte majeure à la vie privée et aux données et des difficultés majeures à atteindre les objectifs peuvent sérieusement nuire à la crédibilité lorsqu'elles se produisent, comme l'ont illustré les récentes commissions royales dans les secteurs des services financiers et des soins aux personnes âgées.

Numérique

Les technologies numériques transforment la société et les marchés. L'intelligence artificielle, la reconnaissance faciale et d'autres innovations pourraient être de plus en plus intégrées aux services et processus gouvernementaux. Ces technologies offrent de vastes possibilités, mais aussi des risques importants.

La numérisation croissante de la société et des entreprises expose également les entreprises aux violations de données et aux cyberattaques.

Les organisations sont vulnérables aux cybercriminels. Les pertes dues aux cyberattaques ont été estimées Selon le Centre australien de cybersécurité, les investissements dans tous les secteurs d'activité en Australie ont atteint 33 milliards de dollars au 30 juin 2021, soit une augmentation de 13 % par rapport à l'année précédente. Un nombre croissant d'initiatives réglementaires sont axées sur le risque cybernétique.

Cependant, les échecs de gestion des risques numériques ne sont souvent pas imputables aux cybercriminels. Des migrations mal planifiées vers de nouvelles plateformes technologiques, des contrôles internes inadéquats sur les données privées, le non-respect des protocoles de sécurité par le personnel et les problèmes connexes peuvent avoir des répercussions importantes sur les organisations.

Indépendamment des complexités techniques, les administrateurs doivent comprendre ces risques, rester vigilants et les surveiller de manière proactive. Ils doivent veiller à ce qu'un suivi rigoureux des incidents soit assuré afin d'identifier de manière proactive les problèmes systémiques plus vastes ou les déficiences du système et à ce qu'il n'y ait aucun retard dans l'élaboration et la mise en œuvre de mesures de conformité améliorées une fois qu'une déficience a été identifiée.

Les risques numériques doivent être fermement intégrés dans le cadre de gestion des risques et de gouvernance de l'organisation. Il peut également être bénéfique de renforcer l'expertise du conseil d'administration en matière de technologie, de cybersécurité et de gestion des risques de projet, ou de s'assurer qu'il a accès à des conseils externes dans ces domaines.

ESG

Les actionnaires et les autres parties prenantes exercent une pression croissante pour que les entreprises prennent des mesures en matière d'ESG, en particulier en ce qui concerne les questions liées au changement climatique. Les administrateurs doivent être conscients des sources de ces pressions et veiller à ce que ces risques soient pris en compte dans le cadre de gestion des risques et de gouvernance de l'organisation.

suite →

Clinique

La Commission royale sur la qualité et la sécurité des soins aux personnes âgées a signalé que les conseils d'administration des prestataires de soins aux personnes âgées doivent être davantage responsables de la fourniture de normes de qualité élevées et de la qualité des soins aux Australiens âgés.

La gestion des risques cliniques concerne la qualité et la sécurité des services de santé, y compris dans les établissements de soins pour personnes âgées.

De nombreuses organisations concernées ont mis en place des processus structurés de gestion des risques. Toutefois, leur mise en œuvre peut présenter des faiblesses à différents niveaux, comme des rapports sporadiques du personnel de première ligne, des réponses inadéquates de la part des supérieurs hiérarchiques et un manque de remontée des informations à la haute direction et au conseil d'administration.

Les conseils d'administration de l'ensemble du secteur de la santé sont encouragés à examiner le rapport final de la Commission royale sur les soins aux personnes âgées et à réfléchir à la manière dont ses conclusions peuvent être appliquées à leurs propres cadres de gestion des risques et de gouvernance.

Les conseils d'administration des établissements de santé ont également l'occasion de tirer les leçons de la pandémie de COVID-19.

Récupération de la Pandémie de covid-19

La reprise après la pandémie de COVID-19 implique de faire face à une série de menaces et de perturbations, notamment :

- chaînes d'approvisionnement – les organisations de tous les secteurs ont été touchées par les perturbations de la chaîne d'approvisionnement, souvent en raison de fermetures de frontières locales ou mondiales et de restrictions de « rester à la maison ». Les impacts à long terme sont encore incertains
- de nouveaux modèles de travail – les employés de nombreux secteurs ont adopté de nouvelles méthodes de travail et l'impact sur les organisations et sur les grands centres urbains reste encore flou
- la rupture de la cohésion sociale, la perturbation des moyens de subsistance et la détérioration de la santé mentale sont ont été signalées lors du Forum économique mondial de 2022 comme des menaces émergentes au cours des deux prochaines années – la lutte contre ces menaces nécessitera probablement des efforts concertés des secteurs privé et public, et
- Alors que de nombreuses organisations ont été affectées négativement par la pandémie de COVID-19, beaucoup d'autres ont trouvé des opportunités importantes, telles que l'innovation dans les produits et les processus qui ont ouvert de nouveaux marchés, une augmentation rapide de l'utilisation de la technologie dans l'ensemble des organisations où, dans des circonstances normales, ces déploiements auraient impliqué des projets pluriannuels et une plus grande volonté organisationnelle d'agir rapidement conduisant à une efficacité accrue.

Les administrateurs doivent prendre en compte l'impact à court et à long terme du COVID-19 sur leurs organisations.

Questions à poser aux administrateurs sur les risques non financiers :

- Tous les risques non financiers importants sont-ils intégrés dans l'élaboration de la stratégie et dans le cadre de gestion des risques ?
- Qui dans l'équipe de direction, les délégations cadre et « trois lignes de défense » est responsable et redevable de la gestion des risques non financiers ?
- Avons-nous besoin de faire appel à une expertise interne et externe pour aider à la gestion des risques non financiers ?
- Quelles technologies numériques émergentes peuvent être intégré à la stratégie et au modèle d'affaires de l'organisation dans le cadre de l'appétence au risque existante ?
- L'appétence au risque de l'organisation doit-elle être ajustée pour refléter l'évolution de l'environnement des risques non financiers ?
- Comment pouvons-nous tirer parti des technologies numériques émergentes telles que le big data, le traitement du langage naturel et l'automatisation des processus robotisés pour améliorer la gestion des risques de l'organisation ?
- Divulguons-nous adéquatement les données environnementales? y compris les risques climatiques, sociaux et de gouvernance pour nos investisseurs et autres parties prenantes ?
- Sommes-nous conscients de l'ampleur de tout risque potentiel harcèlement au travail, intimidation et agression sexuelle dans notre organisation ?
- Évaluons-nous le risque d'esclavage moderne dans nos chaînes d'approvisionnement ?

Quand la gestion des risques échoue

Les sections précédentes de ce guide se sont concentrées sur la manière dont les administrateurs et les conseils d'administration peuvent développer une plus grande maturité face aux risques, afin d'éviter des pertes majeures et des échecs organisationnels.

Une autre question importante pour tout directeur est de savoir quoi faire lorsque la gestion des risques échoue, que la menace se matérialise et qu'un objectif est compromis.

Outre les dommages considérables qu'ils peuvent causer à une organisation et à ses parties prenantes, les échecs en matière de gestion des risques sont de précieuses opportunités d'apprentissage – mais ces leçons peuvent être perdues en raison d'une accusation réciproque ou d'une réticence ou incapacité à identifier les causes profondes.

Enquête approfondie et impartiale

Comme indiqué précédemment dans ce guide, le conseil d'administration doit superviser un processus de surveillance et d'amélioration continue du cadre de gestion intégrée des risques.

Toutefois, un incident ou une crise, en particulier s'il suscite un intérêt public important, peut justifier une approche plus forte.

En règle générale, une première étape bénéfique en réponse à un tel événement à risque est de commander une enquête.

Le conseil d'administration devra soigneusement réfléchir à la conception de cette enquête. La nomination de la personne ou de l'équipe appropriée, interne ou externe à l'organisation, sera fondamentale pour sa réussite. Cette personne ou cette équipe doit avoir suffisamment d'ancienneté et d'indépendance pour être en mesure de fournir des conclusions précises sans influence indue de parties de l'organisation qui pourraient avoir été impliquées dans l'événement à risque.

Il peut sembler qu'une partie externe soit la mieux placée pour cette tâche. Cependant, le conseil d'administration doit tenir compte de la personne à laquelle cette partie externe rend compte au sein de l'organisation, de ses relations antérieures potentielles avec des parties prenantes internes et de ses éventuelles relations commerciales, actuelles ou futures, avec l'organisation qui pourraient affecter son impartialité. Une personne interne ou une unité commerciale de confiance peut être en mesure d'accomplir cette tâche.

Le conseil d'administration devrait tenir compte de sa propre implication dans le risque. événement et sa capacité à être impartial dans la commande de l'enquête.

Au minimum, la personne ou l'équipe chargée de l'enquête doit interroger un large éventail de parties prenantes de l'organisation afin d'identifier les causes profondes qui ont conduit à l'événement.

Le conseil doit déterminer à l'avance le processus de réponse aux conclusions de l'enquête afin de préserver l'indépendance, en particulier si les conclusions peuvent concerner le conseil lui-même.

Assainissement

Une fois les conclusions de l'enquête rendues, le conseil d'administration doit s'assurer que la direction s'attaque rapidement aux causes profondes identifiées, et pas seulement à l'événement isolé.

Si nécessaire, il peut être approprié de collaborer avec les régulateurs sur la mise en œuvre des conclusions.

La réponse du conseil d'administration aux problèmes systémiques devrait envoyer des signaux forts à la direction et au personnel quant à ses attentes en matière de gestion de tout incident futur.

Il convient de tenir compte de la responsabilité et de l'obligation de rendre compte de la haute direction, y compris de tout impact potentiel sur les incitations en matière de rémunération et la longévité du mandat.

Les administrateurs doivent également être conscients que les conclusions récentes des commissions royales ont souligné que les conseils d'administration seront tenus responsables en dernier ressort des événements à risque importants.