RISK IN FOCUS 2019

LES SUJETS INCONTOURNABLES DE L'AUDIT INTERNE

ECIIA

EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING

ifaci

institut français de l'audit et du contrôle internes

TABLE DES MATIÈRES










AVANT-PROPOS

Cette troisième édition de « Risk in focus » est encore plus ambitieuse. Elle est le fruit de la collaboration de sept instituts européens d'auditeurs internes (Allemagne, France, Espagne, Italie, Pays-Bas, Royaume Uni et Irlande, Suède).

Tout comme les années précédentes, nous avons mené une enquête qualitative sur les domaines de risques prioritaires sur lesquels les plans d'audit 2019 devaient porter. Nous avons interrogé des responsables de l'audit interne de ces pays et d'un large éventail de secteurs d'activité.

Cette année, pour la première fois, nous avons également lancé un sondage afin de compléter les entretiens. Nous avons reçu 311 réponses. Ce volet quantitatif a permis d'enrichir ce rapport avec des données sur les risques les plus importants auxquels les organisations sont confrontées selon les responsables d'audit interne et le temps passé par leur fonction sur ces sujets.

Les instituts européens porteurs de ce projet sont très reconnaissants envers tous ceux qui y ont contribué. Nous remercions les quelque 300 responsables de l'audit interne qui ont répondu à notre enquête. Nous apprécions particulièrement le temps consacré par les 42 professionnels que nous avons interviewés. Ce rapport n'aurait jamais vu le jour sans leurs points de vue.

Septembre 2018

LES SUJETS INCONTOURNABLES POUR L'AUDIT INTERNE

L'objectif de « Risk in focus » est de servir de repère pour la profession d'audit interne afin d'aider les responsables d'audit à comprendre la manière dont leurs pairs perçoivent le panorama actuel des risques. Dans la mesure où elle travaille en étroite collaboration avec les conseils, les comités d'audit et les autres parties prenantes, la fonction d'audit interne devrait déjà avoir une image claire de l'organisation et des principaux risques financiers, opérationnels et stratégiques auxquels elle est confrontée. Il est toutefois essentiel que la profession partage cette connaissance et ces réflexions afin de renforcer les évaluations et la cartographie des risques et, finalement, fournir une meilleure assurance.

Alors que de nombreuses fonctions d'audit interne se concentreront sur des missions d'audit opérationnel, et que toutes devraient être focalisées sur des missions d'assurance spécifiques à leur organisation, les sujets incontournables proposés dans ce rapport reflètent des thèmes pertinents pour l'ensemble des secteurs d'activité, en mettant l'accent sur les risques nouveaux et émergents. Cette liste n'a évidemment pas pour vocation d'être exhaustive, et nous attendons de l'audit interne qu'il adopte une approche fondée sur les risques en se concentrant sur les risques prioritaires auxquels son organisation doit faire face. Ces sujets doivent donc être pris comme des points de repère lors de l'élaboration du plan d'audit.

Les fonctions d'audit les plus matures ne se contenteront pas de tester les dispositifs existants de contrôle interne, mais elles aideront également leur entreprise à identifier les risques qui se profilent à l'horizon. Nous espérons donc que ces sujets incontournables constitueront une ressource précieuse qui permettra aux responsables de l'audit interne d'évaluer les risques qui n'ont pas encore été pris en compte, ou d'envisager sous un angle nouveau les risques déjà surveillés. Certains lecteurs retrouveront des thèmes de leurs propres évaluations des risques, et ils devraient s'en réjouir. Cela confirme qu'ils sont conscients des risques encourus. D'autres considéreront que les sujets mis en évidence pourront les aider à élaborer leur plan d'audit pour l'année à venir.

Comme l'année précédente, nous avons interviewé des responsables d'audit interne à travers l'Europe. Ces opinions viennent compléter le sondage (voir ci-dessous) que nous avons entrepris et qui nous permet de présenter les risques prioritaires auxquels les organisations sont confrontées, tels qu'identifiés par leurs responsables de l'audit interne. Les entretiens nous ont permis d'approfondir et d'attirer l'attention sur des problématiques plus épineuses liées à ces grands facteurs de risques prioritaires.

Dans la plupart des cas, notre sondage portant sur différents pays et secteurs n'a pas révélé de divergences notables à propos des principaux risques identifiés par les responsables de l'audit interne. Nous avons toutefois constaté que les Pays-Bas étaient le seul pays dans lequel la culture était considérée, sur une base cumulée, comme représentant le plus grand risque pour les organisations. Cette évaluation est en cohérence avec l'introduction de la culture en tant qu'élément d'une gouvernance efficace lors de la révision du Code de gouvernance d'entreprise qui est entré en vigueur début 2018 dans ce pays.

De même, nous avons constaté que la moitié des Néerlandais interrogés soulignaient l'importance des enjeux de développement durable liés à l'éthique environnementale et sociale. Cela pourrait être également lié à la révision de ce Code de gouvernance. En effet, l'un des deux principaux changements mettaient l'accent sur la création de valeur à long terme, un élément explicitement lié aux « questions environnementales, sociales et salariales ». Nous avons également remarqué que deux tiers des Français interrogés soulignaient l'importance d'un programme de conformité anti-corruption, un taux plus élevé que dans tous les autres pays. Ce constat est sans doute lié à l'application de la loi Sapin II dans le pays.

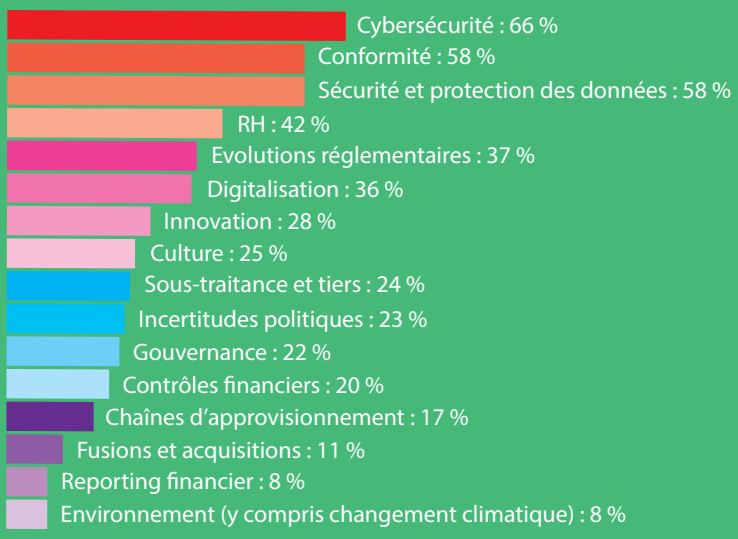
Nous avons conscience des limites d'une analyse qualitative basée sur un échantillon de 42 responsables de l'audit interne répartis sur sept pays, et nous savons à quel point il est difficile de lui attribuer un caractère significatif. Nous demandons donc aux lecteurs de tirer leurs propres conclusions de ces observations. De plus, nous ne suggérons aucunement que les organisations d'autres pays devraient traiter avec une moindre priorité les questions de conformité anti-corruption ou les risques liés au développement durable.

Nous espérons que vous apprécierez cette édition de « Risk in focus ». Comme toujours, vos réactions sont les bienvenues et nous vous remercions de votre intérêt.

Quel est le principal risque auquel votre organisation est confrontée ?

- Cybersécurité : 15 %
- Conformité : 13 %
- Digitalisation : 9 %
- Evolutions réglementaires : 8 %
- Incertitudes politiques : 8 %
- Sécurité et protection des données : 6 %
- Culture : 6 %
- RH : 5 %
- Innovation : 5 %
- Gouvernance : 3 %
- Sous-traitance et tiers : 3 %
- Contrôles financiers : 3 %
- Chaînes d'approvisionnement : 2 %
- Fusions et acquisitions : 1 %
- Reporting financier : 1 %
- Environnement (y compris changement climatique) : 1 %
- Autre (non précisé) : 11 %

Lequel de ces domaines fait partie des cinq principaux risques auxquels votre organisation est confrontée ?



CYBERSÉCURITÉ : GOUVERNANCE DES SI ET RELATIONS AVEC LES TIERS

La cybersécurité est un risque hautement prioritaire depuis des années, et ce sans aucun signe d'atténuation. Les entreprises s'efforcent de se défaire de leurs vieux systèmes et, à mesure que la maturité de la gestion des cyber-risques progresse, l'attention se tourne vers la robustesse de la protection des tiers.

Les entretiens, que nous avons réalisés auprès de plus de 300 responsables de l'audit interne, montrent que la cybersécurité est, à leurs yeux, le principal risque pour leur organisation. Pour les deux tiers d'entre eux, la cybersécurité fait partie des cinq principaux risques, et pour 15 % des sondés, il s'agit du risque le plus important, devant la conformité (13 %), la digitalisation (9 %), les évolutions réglementaires (8 %) et les incertitudes politiques (8 %). Comme on pouvait s'y attendre, notre enquête qualitative souligne que l'ensemble des responsables de l'audit interne ont prévu de prendre en compte cette problématique, sous une forme ou une autre, pour leurs plans d'audit 2019, reflétant ainsi les observations de nos rapports précédents.

Qu'on la nomme cybersécurité, sécurité des SI, sécurité de l'information, ou autrement, la nécessité de défendre les réseaux et les données qui s'y trouvent fait désormais partie du paysage. La sophistication des attaques, provenant parfois de certains Etats, et l'évolution constante de la menace a engendré une course entre les auteurs de menaces et les professionnels de la sécurité des systèmes d'information.

L'approche fragmentée adoptée par les entreprises au cours des dernières décennies concernant la planification et le développement de l'infrastructure de leurs systèmes d'information est un obstacle majeur à l'atténuation de ce risque. La gouvernance et la surveillance insuffisantes des SI, à une période où les cyber-risques étaient faibles, a abouti à des systèmes cloisonnés et des réseaux partiellement verrouillés. Maintenant que la cyber-criminalité explose - il est prévu que le coût des dommages causés par ce type d'attaques double entre 2015 et 2021 pour atteindre 6 000 milliards de dollars [1] - il est difficile de défendre ces systèmes hétérogènes.

Les premières étapes de la migration des anciens systèmes (tels que Windows 98, NT et 2000 et les logiciels non pris en charge, y compris Internet Explorer 7, 8, 9 et 10) et de la rationalisation des infrastructures des systèmes d'information sont en cours, et la valeur des tests de pénétration et de l'*ethical hacking* (piraterie éthique) est dorénavant bien comprise. À mesure que ces systèmes sont mis aux normes, que la maturité de la gestion des cyber-risques progresse, les entreprises sont mieux à même de maîtriser les menaces qui pèsent sur leurs opérations directes. L'attention se déplace donc vers l'extérieur.

Chaînes d'approvisionnement et *cloud*

De nos jours, les hackeurs ne se contentent plus de viser directement les organisations, ils tentent également de les atteindre par le biais de leurs principaux fournisseurs et partenaires en technologie. L'an dernier, l'attaque de Petya, l'une des plus importantes à ce jour, a utilisé cette méthode en exploitant le logiciel de comptabilité ukrainien MeDoc comme point d'entrée pour exécuter un code malveillant qui s'est ensuite propagé sur les réseaux d'entreprise du monde entier. Cet exemple emblématique n'a pas été un cas isolé ; selon les estimations, l'incidence des programmes malveillants introduits dans les chaînes d'approvisionnement afin d'infiltrer discrètement leurs cibles a augmenté de 200 % en 2017 [2]. La nature interconnectée et interdépendante des activités qui nous entourent, et les nouvelles stratégies de piratage cherchant à s'infiltrer dans ce réseau de relations multiplient la probabilité de cyberattaques. Ainsi, la force des organisations se mesure au niveau du maillon le plus faible de leurs chaînes d'approvisionnement.

L'intégrité des services hébergés dans le *cloud* (informatique dans les nuages) est un autre élément à prendre en considération. La migration de certains services et de certaines données sur le cloud est souvent motivée par un solide *business case*. Elle peut en effet permettre de réduire les coûts des matériels et des logiciels, ainsi que d'autres frais généraux, et faciliter le travail à distance, la collaboration et la reprise après sinistre. Les prestataires du *cloud* hébergent une immense quantité de données pour leurs clients, et les principaux fournisseurs de services numériques, comme Google (Google Cloud Platform), Amazon (AWS) et IBM/ Microsoft (Azure), emploient les meilleurs experts disponibles afin d'assurer la sécurité de leurs plateformes et s'appuient sur des systèmes automatisés capables de détecter et de bloquer quotidiennement des millions d'attaques liées aux mots de passe.

Toutefois, en 2017, Microsoft a rapporté que le nombre d'attaques sur les comptes *cloud* de ses clients avait quadruplé en une année. L'entreprise a remarqué que la majorité des menaces résultaient de mots de passe vulnérables, faciles à deviner et mal gérés, suivis d'attaques de hameçonnage *(phishing)* ciblées et d'intrusions chez des tiers. L'incident dont FedEx a été victime en 2017 illustre bien ce propos ; l'entreprise a perdu 300 millions de dollars de chiffre d'affaires lorsque ses données ont été volées sur un serveur hébergé par Amazon. Les recherches ont ensuite montré que le serveur *cloud* n'était pas protégé par un mot de passe. Cela démontre toute l'importance pour les organisations d'appliquer le même niveau de contrôle des systèmes de sécurité sur toutes leurs infrastructures SI, qu'elles soient internes ou externes.

66 % des responsables de l'audit interne déclarent que la cybersécurité est un des cinq principaux risques auxquels les organisations sont confrontées.

Source : Sondage réalisé auprès de nos membres

« Nous menons un **audit conjoint** avec dix banques chez un de nos fournisseurs de services *cloud*, Microsoft Azure, afin d'obtenir l'assurance que nous cherchons tous. C'est une **avancée majeure** ; c'est la première fois que nous participerons à une telle mission. Les **prestations externalisées** ont toujours posé problème, car les tiers ne peuvent pas gérer l'afflux de chacune des 10 fonctions d'audit, et il leur est souvent **impossible** de délivrer des rapports d'assurance **sur-mesure** pour chacun de leurs clients ».

Responsable de l'audit interne, groupe bancaire multinational, Pays-Bas

« Compte tenu de la **croissance** de l'entreprise et de la quantité de données que nous détenons, les cyber-risques sont **de plus en plus importants.** Il existe des menaces externes, mais comment s'assurer que les prestataires détiennent **assez de données** pour soutenir l'activité, tout en respectant les limites nécessaires pour la confidentialité ? Nous avons d'excellents contrats, mais plus personne ne les consulte. Il est utile **d'examiner régulièrement les macro-processus** et les **risques** auxquels les fournisseurs de service nous exposent. Nous n'avons pas fait grand-chose dans ce domaine, et la **gestion des fournisseurs** est un de nos thèmes pour 2019 ».

Responsable de l'audit interne, groupe de distribution multinational, Pays-Bas

56 %

des organisations ont été touchées par une faille provenant d'un de leurs fournisseurs en 2017. Cela représente une hausse de 6 % par rapport à l'année précédente

Source : Ponemon Institute

L'incidence des programmes malveillants introduits dans les chaînes d'approvisionnement afin d'infiltrer discrètement les organisations a augmenté de **200 %** en **2017**

Source : Symantec

Le coût des dommages causés par des cyber-attaques devrait doubler entre 2015 et 2021 pour atteindre **6 000 milliards de dollars**

Source : Cybersecurity Ventures

L'intérêt porté aux cyber-risques liés aux tiers est particulièrement pertinent au regard du Règlement général européen sur la protection des données (RGPD). Le RGPD prévoit que les « responsables du traitement » et les « sous-traitants » sont conjointement et solidairement responsables lorsqu'ils portent tous deux la faute des dommages causés par le traitement des données. Par conséquent, si une organisation stocke dans le *cloud* des données à caractère personnel de citoyens européens et que son prestataire est victime d'une violation des données, cette organisation, en tant que responsable du traitement, peut être tenue responsable de cette défaillance à condition que le sous-traitant ait respecté les exigences fixées dans le contrat/accord de partage. De plus, bien que l'attention et les préoccupations se soient principalement portées sur l'amende pouvant être imposée par les organismes de contrôle en vertu du RGPD, ces organismes ont aussi le pouvoir de stopper tout traitement en cas de violation. Cette mesure peut potentiellement geler les opérations d'une entreprise en raison d'un incident survenu au niveau du fournisseur de services *cloud*, quel que soit le responsable, une telle perturbation pouvant entraîner d'importantes pertes.

« Des entreprises comme Amazon proposent des solutions de stockage dans le *cloud*, mais en termes de contrôle interne et de gestion des fournisseurs, ces prestataires ont des clauses d'audit bien plus contraignantes que les autres. C'est devenu une préoccupation majeure après la fuite de données qui a touché Facebook. Nous essayons donc de revenir aux fondamentaux en examinant le registre des prestataires, leurs plans de gestion des risques et en particulier le niveau de précision de ces plans. La manière dont l'organisation met œuvre le suivi des prestataires constituera un point central de nos plans d'audit à l'avenir ».

Responsable de l'audit interne,
groupe bancaire multinational, Espagne

Du point de vue de l'audit interne

Les cyber-risques font désormais partie du paysage et la troisième ligne de maîtrise devra fournir une assurance concernant la gestion interne de ce risque dans les limites d'un horizon de temps prévisible voire indéfini. Mettre correctement en place les dispositifs essentiels au niveau des pare-feu, sécuriser les configurations, la gestion des patchs, le contrôle des accès et la protection contre les programmes malveillants reste de la plus haute importance. De plus, ces dispositifs de contrôle devront certainement faire l'objet d'une évaluation régulière. Il en est de même pour les tests de pénétration, mais compte tenu de la probabilité d'une faille, il sera tout aussi important que les professionnels de la sécurité des SI effectuent un contrôle et une détection en continu.

L'évaluation de la gouvernance de ce domaine sera également très utile. En effet, les systèmes d'information sont trop souvent considérés comme indépendants des métiers. Par le passé, la construction du réseau et des systèmes de l'organisation a pu être gérée avec une très grande autonomie, provoquant d'importants problèmes de sécurité à long terme. L'audit interne pourra décider d'attirer l'attention de la direction générale sur cette question et, si nécessaire, recommander une meilleure supervision des décisions d'achat ainsi qu'une approche plus stratégique et prospective dans le développement des systèmes d'information de l'organisation afin d'éviter les infrastructures fragmentées susceptibles d'être exposées à un plus grand nombre de vulnérabilités et de points d'entrée potentiels. L'an dernier, la Confédération européenne des instituts d'audit interne et la Fédération des associations européennes de gestion des risques ont publié un rapport commun, *« At the junction of corporate governance and cybersecurity »,* qui souligne le besoin d'ajuster les stratégies de management des cyber-risques avec les objectifs et stratégies de l'organisation.
Le rapport peut être consulté ici : bit.ly/ECIIAcyber

Avec la multiplication des attaques visant les principaux fournisseurs de services *cloud*, comme Microsoft, l'organisation devrait vérifier, en interne, que les cyber-risques encourus par les tiers sont contrôlés conformément aux mêmes normes que celles appliquées au sein de l'entreprise, y compris les fondamentaux tels que la gestion des mots de passe. Ceci peut impliquer d'identifier les tiers chargés des principaux services informatiques, de s'assurer qu'ils sont contrôlés et évalués plus fréquemment que les autres, de vérifier que les fournisseurs de services *cloud* respectent le RGPD, d'exercer la clause d'audit pour tester la robustesse de leurs systèmes de contrôle, d'évaluer les processus de diligence raisonnable lorsque de nouveaux fournisseurs sont engagés, et de mener des recherches indépendantes sur la réputation des tiers sur le marché.

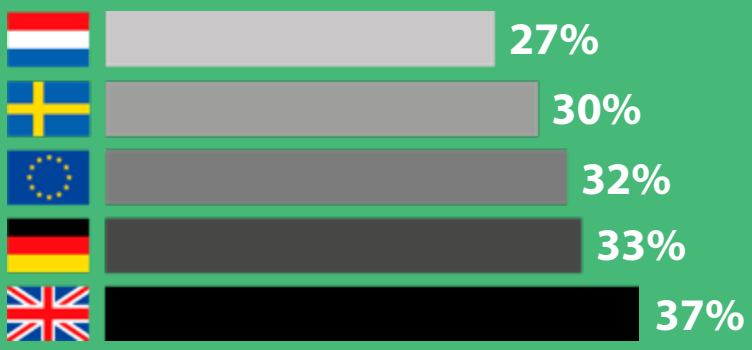
Questions clés

- L'organisation a-t-elle engagé une migration de ses vieux systèmes ou a-t-elle déjà un système plus homogène et équilibré qui soit plus facile à défendre ?
- La sécurité est-elle un élément essentiel de la planification des systèmes d'information et du développement du réseau ?
- Existe-t-il une gouvernance forte en matière de systèmes d'information et une surveillance des achats et du développement des réseaux ainsi que de l'infrastructure ?
- En plus de solides défenses lui permettant d'éviter les intrusions, l'organisation déploie-t-elle des moyens de surveillance efficaces lui permettant de détecter les incidents ?
- La gestion interne des cyber-risques est-elle suffisamment mature pour que l'attention nécessaire puisse être portée sur les tiers ?
- Quels services *cloud* l'entreprise utilise-t-elle et comment s'assure-t-elle que ces prestataires respectent des normes de sécurité élevées et maintiennent des dispositifs de contrôle solides ?
- Les normes appliquées en interne concernant la gestion des mots de passe sont-elles également suivies pour les services *cloud* ?
- Quelle est la robustesse des processus de diligence raisonnable de la fonction achat en matière de cybersécurité lors de la prise de contact et de l'engagement des fournisseurs et des partenaires commerciaux ?

« La **tendance est clairement** au ***cloud*** et à la virtualisation des serveurs, mais je pense que peu de responsables d'audit savent réellement où en est la fonction SI et quels sont les dispositifs de contrôle en place.
La plupart des fonctions SI **ont une gouvernance insuffisante** ; dans la majorité des organisations, il n'existe pas une gouvernance efficace des systèmes d'information. En tant que responsables de l'audit interne, nous apportons différentes pièces à l'édifice, mais nous ne saisissons pas vraiment comment elles s'intègrent à l'organisation.
Il est donc nécessaire de **surveiller davantage** les évolutions informatiques majeures et de mieux comprendre comment les dispositifs de contrôle se positionnent entre l'organisation et ses prestataires de *cloud*.
De manière plus générale, nous n'avons pas encore tout à fait saisi ce qu'une **bonne gestion** des capacités SI signifiait ».

Responsable de l'audit interne,
secteur public, Royaume-Uni

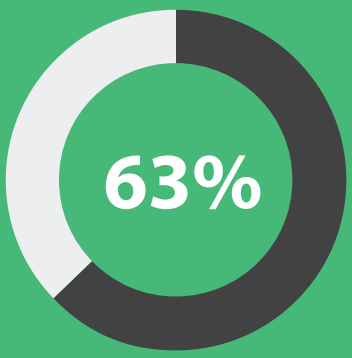
Entreprises ayant subi une fuite de données en 2017, en pourcentage



Source : Thales Security

Microsoft a indiqué que les cyber-attaques à l'encontre de ses services *cloud* avaient quadruplé en 2017

Source : Rapport Microsoft Security Intelligence



63 % des failles peuvent être imputées à des fournisseurs tiers

Source : Soha System

« Nos systèmes d'information ont été développés au cours des 20 dernières années, à une époque où la **cyber-menace** n'existait pas. Ces **systèmes intégrés** souffrent donc d'une sécurité insuffisante. Si un rançongiciel prenait en otage notre organisation, il faudrait beaucoup de temps pour remettre en état nos **infrastructures** matérielles, ce qui pourrait constituer une menace pour la sécurité des personnes. L'attention de l'audit interne est passée de l'efficience et des opérations aux **questions de base liées à la sécurité** ».

Responsable de l'audit interne,
secteur public, Suède

PROTECTION DES DONNÉES : STRATÉGIES POST-RGPD

Le délai pour mettre en place le Règlement général de l'Union européenne sur la protection des données (RGPD) est arrivé à échéance. Les fonctions d'audit interne ont déjà examiné le niveau de préparation à la conformité ou s'apprêtent à le faire très rapidement. Mais les enjeux vont bien au-delà d'une simple case à cocher concernant la conformité au RGDP.

Les discussions qui ont entouré le RGPD au cours des 18 derniers mois ont fait beaucoup de bruit, ce qui est peu surprenant compte tenu de la portée de cette réglementation (elle s'applique à toutes les entreprises traitant des données à caractère personnel de citoyens européens), de sa neutralité sectorielle et des lourdes amendes qui sanctionneraient une non-conformité. Nous avions déjà mentionné le défi que représentait cette réforme radicale dans notre précédent rapport et, cette année encore, toutes les personnes interrogées dans le cadre de notre enquête qualitative ont mentionné la conformité au RGPD, ou plus généralement la problématique de la sécurité des données, de la gouvernance et des stratégies y afférentes, comme un risque à cibler pour 2019 et les années à venir. À l'appui de ce constat, notre sondage a révélé que 58 % des sondés plaçaient la conformité parmi les cinq risques les plus importants de leur organisation juste derrière la cybersécurité (66 %)

L'Europe n'est pas le seul territoire à renforcer sa réglementation ; le 1er mai, la Chine a publié ses directives en matière de sécurité des données personnelles *(Personal Information Security Specification)* qui fournissent des lignes directrices détaillées quant à la conformité à la loi sur la cybersécurité du pays, adoptée en 2016. Ces lignes ont largement été inspirées par le RGPD, les entreprises déjà en conformité avec la réglementation européenne ont donc de grandes chances de satisfaire aux normes chinoises, mais elles devraient tout de même effectuer une analyse des écarts avec ces directives si elles sont inquiètes quant à l'utilisation qu'elles font des données personnelles des citoyens chinois.

Les questions de réputation

Le RGPD a eu un important effet domino. Lorsque la loi est entrée en vigueur le 25 mai, Facebook, une des entreprises traitant le plus de données au monde, a demandé à ses 2,2 milliards d'utilisateurs de revoir leurs paramètres de sécurité, sans même y être contrainte. La crise de confiance qui avait touché le média social n'y est certainement pas étrangère.

En effet, début 2018, Facebook a été sévèrement affecté quand il est apparu que le cabinet de conseil Cambridge Analytica avait récolté plus de 87 millions de données d'utilisateurs pour soutenir la campagne présidentielle de Donald Trump lors des élections de 2016.

Le Bouclier de protection des données UE - États-Unis

Le RGPD mentionne un certain nombre de conditions concernant le transfert des données personnelles hors de l'Union Européenne. L'une d'entre elles exige que les données ne doivent être transférées que vers des pays dont la législation en matière de protection des données est jugée suffisante.

Actuellement, le niveau de protection des données aux États-Unis ne respecte pas cette exigence. Néanmoins, le Bouclier de protection des données entre l'Union Européenne et les États-Unis *(EU-US privacy shield scheme)* autorise les entreprises nord-américaines certifiées et ayant les dispositifs de contrôle appropriés, à recevoir des données personnelles provenant de l'Europe.

Cependant, un groupe de parlementaires européens souhaite que cet accord soit suspendu. Ils considèrent qu'il ne fournit pas les garde-fous nécessaires et ne devrait être activé que lorsque ces insuffisances auront été traitées. Les entreprises européennes qui partagent des données personnelles avec des partenaires commerciaux américains devraient être attentives aux évolutions dans ce domaine.

Pour plus d'informations, rendez-vous sur www.privacyshield.gov

Après la révélation de cette affaire, la valeur boursière de l'entreprise a chuté de 70 milliards de dollars en dix jours. Le cours des actions de l'entreprise s'est rétabli, mais le scepticisme à l'égard de l'utilisation éthique des données personnelles à des fins commerciales, voire politiques, s'est accru, et les législateurs de différents pays exigent un devoir de rendre compte. Selon une estimation, 60 % des Allemands craignent que Facebook et d'autres réseaux sociaux aient une influence négative sur la démocratie [3], et moins de la moitié des Américains font aujourd'hui confiance à Facebook quant au respect des lois américaines sur la protection de la vie privée [4]. Ceci montre bien que la sécurité des données n'est pas seulement une histoire de conformité, mais une question de confiance et de réputation.

SÉCURITÉ DES DONNÉES : CONFORMITÉ :

58 % des responsables de l'audit interne affirment que la sécurité des données et la conformité font partie des cinq principaux risques auxquels leur organisation est confrontée

Source : Sondage réalisé auprès de nos membres

« Le **RGPD** va être au programme pendant un long moment ; il touche toutes les entreprises. Il nécessite une plus grande **confidentialité des données** et une amélioration de la gestion des données, non seulement du **point de vue de la réglementation,** mais aussi pour s'assurer de la **confiance des consommateurs.** De plus, si nous possédons un grand nombre de données, à quoi peuvent-elles servir ? Quelles opportunités pouvons-nous en tirer ? »

Responsable de l'audit interne, groupe de télécommunications, Suède

« Vous avez une **meilleure visibilité** sur la gestion des données personnelles lorsque vous ne vous arrêtez pas au RGPD, mais que vous considérez la confidentialité et la **gestion de données** comme un tout. Avec les problèmes au niveau des médias sociaux, il ne fait aucun doute que la question va continuer à se poser.
Et cela se **transforme** en un phénomène plus **général**, qui englobe la manière dont les organisations gèrent les données, particulièrement les **données fournies par des tiers,** ainsi que les risques qui peuvent y être associés ».

Responsable de l'audit interne, établissement financier, Royaume-Uni

50 %

Dans le sillage du scandale sur la gestion des informations personnelles, moins de 50 % des Américains font confiance à Facebook quant au respect des lois en matière de protection des données personnelles

Source : Reuters/Ipsos

60 %

des Allemands affirment craindre que Facebook et d'autres médias sociaux aient un impact négatif sur la démocratie

Source : Bild am Sonntag

27 %

27 % seulement des entreprises européennes déclaraient respecter le RGPD un mois après sa mise en application le 25 mai 2018

Source : TrustArc

74 %

Toutefois, 74 % prévoyaient de se mettre en conformité d'ici fin 2018, et 93 % d'ici fin 2019

Source : TrustArc

« Nous allons focaliser notre attention sur la conformité au RGPD. Nous avons déjà abordé ce domaine cette année en nous intéressant à la conformité au RGPD de l'organisation et de ses produits. Nos clients s'attendent à ce que nos produits soient conformes. Des lois similaires sont en train d'être adoptées dans d'autres pays, par exemple, en Chine et en Russie. Ce thème reste donc dans la cible des auditeurs internes. Il ne s'agit pas que du RGPD, mais de la protection des données, sous toutes ses formes, et dans divers territoires ».

Responsable de l'audit interne, éditeur de logiciels multinational, Allemagne

Stratégie et gouvernance

Le respect du RGPD est sans aucun doute une préoccupation majeure, mais il ne suffit pas d'être en totale conformité avec la loi le jour de son entrée en vigueur, puis de l'oublier ensuite. En effet, les données, qu'elles soient personnelles ou organisationnelles, ne sont pas seulement d'une grande valeur, elles se multiplient également de manière exponentielle.

On estime ainsi que le trafic sur Internet a dépassé le zettaoctet en 2016, l'équivalent de 150 millions d'années de streaming vidéo en haute définition, ce chiffre étant supposé tripler d'ici 2021 [5]. Les données ont d'autant plus de valeur que leur analyse et les perspectives que les entreprises peuvent en déduire sont matures. Dans le même temps, puisque la collecte et l'exploitation des données par les entreprises sont en constante évolution, la conformité au RGPD sera nécessairement une cible mouvante qui devra être réexaminée à mesure que de nouvelles applications et utilisations des données personnelles émergeront. La capacité de gérer et de modéliser ces torrents d'informations est essentielle à la réussite de l'entreprise. Les organisations doivent donc développer des stratégies de gestion des données et une gouvernance qui soutiennent plus largement la stratégie de l'entreprise et ses objectifs de création de valeur, tout en maintenant des normes de sécurité et de conformité de haut niveau.

Ainsi, il pourra être envisagé de recruter un CDO *(Chief Data Officer* ou administrateur général des données), un rôle qui s'est développé ces cinq dernières années, et d'établir une fonction de gestionnaire des données qui s'efforcera de standardiser les données non structurées et d'améliorer la gouvernance de leur gestion. Lorsqu'elles ont atteint une certaine maturité au niveau de ces fondamentaux, les entreprises peuvent alors se concentrer davantage sur l'analyse et les techniques de modélisation qui permettent de maximiser la valeur des données qu'elles possèdent, tout en assurant leur sécurité.

Du point de vue de l'audit interne

Si l'audit interne n'a pas encore fourni l'assurance que l'organisation était en conformité avec le RGPD, il est temps d'effectuer cette mission. Pour un grand nombre d'entreprises, en particulier celles pour lesquelles les données personnelles sont au cœur de leur modèle d'affaires, des revues périodiques seront nécessaires, en particulier lorsque de nouveaux points de données ou moyens sont mis en place, par exemple le suivi du comportement des clients par le biais d'une publicité géolocalisée sur les smartphones des utilisateurs.

Au-delà de ce type de mission, la fonction d'audit interne a la possibilité d'évaluer dans quelle mesure l'organisation a établi une stratégie en matière de données ainsi que des règles de gouvernance des données. Cela impliquera de prendre en compte la manière dont les données sont gérées, d'apprécier leur impact réel sur la création de valeur (chiffre d'affaires et bénéfices) et leur capacité à soutenir les objectifs et la stratégie de l'entreprise. Dans la mesure où toute perte de données (que ce soit par des hackers ou des acteurs internes) implique une perte de valeur, la stratégie en matière de données devra être en phase avec la stratégie de cybersécurité de l'organisation.

Adopter un modèle économique fondé sur les données est synonyme de changements importants ; ce processus peut être soutenu par la troisième ligne. Il se peut qu'il n'y ait pas de règles prédéfinies sur lesquelles orienter la mission, et que les détails de ces changements soient peu précis. Toutefois, la mission d'audit interne doit s'en tenir aux principes fondamentaux de la gestion de projet, tels que la clarté des objectifs, la précision des responsabilités et le devoir de rendre compte, l'alignement de la stratégie en matière de données sur la stratégie globale de l'entreprise, la validité des indicateurs clés de performance utilisés pour mesurer la réussite du changement, et l'évaluation de l'impact de ces changements sur les dispositifs de contrôle, les processus, les risques et la structure de l'entreprise.

Questions clés

- L'organisation est-elle en conformité avec le RGPD et, le cas échéant, avec d'autres lois étrangères telles que la loi chinoise sur la protection des données personnelles *(Personal Information Security Specification)* ?
- Les entreprises nord-américaines qui partagent des données avec l'organisation sont-elles certifiées dans le cadre du Bouclier de protection des données UE-États-Unis *(EU-US privacy shield scheme)* ?
- Comment les données personnelles et les données métier ou stratégiques sensibles sont-elles partagées avec les tiers, et comment vous assurez-vous que ces tiers les protègent ?
- La direction générale et, le cas échéant, la fonction de conformité sont-elles conscientes de la nécessité de maintenir la conformité à mesure que l'entreprise et ses modalités de collecte et d'utilisation des données évoluent ?
- Lorsqu'elle existe, la fonction de conformité entretient-elle une communication étroite avec celle qui est en charge du management des données afin d'être informée de la manière dont les changements affectant l'entreprise peuvent avoir un impact sur la conformité au RGPD ?
- Existe-t-il une stratégie régissant la façon dont l'organisation utilise les données, personnelles ou autres, à son avantage ? Est-elle en phase avec sa stratégie globale ?
- Comment la stratégie relative aux données prévoit-elle leur utilisation à l'avenir ? Est-elle claire et bien formulée ?
- La fonction d'audit interne est-elle prête à conseiller le CDO et/ou le gestionnaire des données concernant des changements dans l'utilisation des données en apportant un point de vue en matière de contrôles et de risques ?

En 2012, **12 %** seulement des sociétés classées Fortune 1 000 employaient un CDO ...

... en 2018, **63 %** avaient identifié ce rôle dans leur organisation

Source : NewVantage Partners

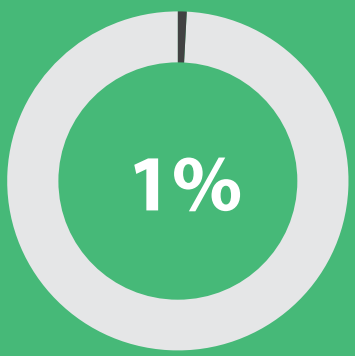
« Ce n'est pas **seulement** une **question de règlementation.** Lorsque vous parlez de fuites de données, la chose la plus importante à nos yeux, ce sont nos clients, et nous sommes très impliqués dans la protection des données personnelles. Nous souhaitons surveiller ces risques non seulement parce que nous risquons une **amende**, mais aussi parce que nous gérons **de plus en plus de données**, et nous devons nous assurer qu'elles sont efficacement protégées. Il faut un **processus continu**, pour être en conformité **aujourd'hui**, et **demain** ».

Responsable de l'audit interne, groupe de médias, France

44
zettabytes

D'ici 2020, le volume cumulé de Big Data (ou « mégadonnées ») sera passé de 4,4 zettabytes à environ 44 zettabytes

Source : Dell EMC



Moins de 1% des données non structurées détenues par les entreprises sont analysées ou utilisées

Source : Harvard Business Review

« Les événements qui ont récemment touché **Facebook** signifient que les organisations doivent se montrer plus transparentes quant à l'utilisation qu'elles font de leurs données et à la manière dont elles les protègent. Ces enjeux sont largement pris en compte par le RGPD, mais la **réglementation** est toujours **à la traîne** de l'évolution du monde réel. L'audit interne doit s'intéresser à la **création de valeur à long terme**. C'est-à-dire être attentif aux valeurs de son organisation et plus généralement aux **valeurs de la société**, pour se demander si certaines activités de l'organisation pourraient ne **pas être acceptées**, même si elles sont légales. Il n'existe aucun manuel ni aucune réglementation pour en juger, mais c'est la fonction d'audit interne qui devrait émettre le **signal d'alerte**, sinon, qui d'autre le fera dans l'organisation ? »

Responsable de l'audit interne, cabinet de prestations externes, Pays-Bas

80 %
du temps des analystes est consacré à la recherche et à la préparation des données plutôt qu'à leur analyse

Source : Harvard Business Review

DIGITALISATION, AUTOMATISATION ET IA : RISQUES LIÉS À L'ADOPTION DES TECHNOLOGIES

Les avantages en termes de coûts et d'efficience de l'automatisation et d'autres processus numériques peuvent être source de transformation s'ils sont exploités à leur plein potentiel. Toutefois, les organisations doivent également prendre en compte les risques associés à de tels changements.

Notre recherche montre que 36 % des responsables de l'audit interne considèrent la digitalisation comme l'un des cinq principaux risques auxquels leur organisation doit faire face, et près d'un sur dix (9 %) le place en tête du classement, juste derrière la cybersécurité (15 %) et la conformité (13 %). Parmi les responsables de l'audit interne interrogés dans le cadre de nos entretiens déclarent que les risques liés à la digitalisation et à l'adoption des technologies constitueront un aspect important de leur travail en 2019 et dans les années à venir.

Le rythme des innovations et la capacité des organisations à suivre celui de leurs concurrents avaient été identifiés dans le rapport de l'année dernière. Ces thèmes restent d'actualité, en particulier dans les secteurs les plus touchés par les technologies, comme les médias, les télécommunications, la banque de détail et d'autres activités en contact direct avec la clientèle. Ces entreprises, qui sont déjà lancées dans l'aventure du numérique, peuvent avoir tendance à se focaliser sur les bénéfices sans tenir entièrement compte des risques auxquels ces technologies les exposent.

Mais qu'entend-on par digitalisation ? C'est un terme générique pour désigner la mise en place de systèmes de centralisation des données et des processus pour la planification des ressources *(Enterprise Resource Planning* ou ERP) et la gestion de la relation client *(Customer Relationship Management* ou CRM), tels que SAP et Salesforce, jusqu'aux technologies automatisées.

Les étapes fondamentales de l'adoption des systèmes ERP et CRM peuvent se révéler extrêmement bénéfiques. Par exemple, en 2009, l'intégration de ces technologies est moins répandue au Royaume-Uni qu'elle ne l'était au Danemark. Un phénomène à associer à l'écart de productivité (la productivité du Royaume-Uni n'a pas connu de croissance depuis 2008). On estime ainsi que l'utilisation d'outils tels que les systèmes ERP et CRM pourrait entraîner une hausse de 100 milliards de livres sterling du produit intérieur brut du Royaume-Uni.

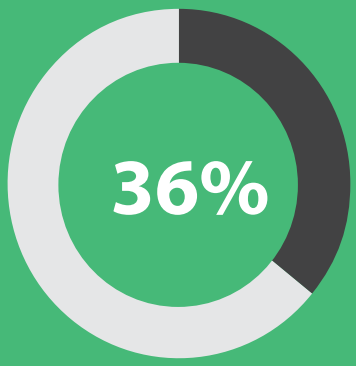
À l'autre extrémité du spectre, on trouve des technologies comme l'automatisation des processus robotisés *(Robotic Process Automation* ou RPA) et l'intelligence artificielle (IA). La RPA passe par l'utilisation d'un logiciel qui automatise un processus selon des instructions de programmation, sans apprentissage. L'IA se réfère quant à elle à des systèmes d'auto-apprentissage par le traitement de données non structurées qui permettent une amélioration de cet apprentissage au fil du temps.

Prise en compte des risques

L'automatisation est déjà une réalité pour bon nombre d'organisations. Les entreprises en contact direct avec les consommateurs ont de plus en plus recours à des *chatbots* pour gérer les questions de leurs clients. Dans la banque de détail et l'assurance, des algorithmes sont utilisés pour rapidement et automatiquement souscrire à des produits financiers. Les bénéfices sont évidents en termes de coût et d'efficience, mais quels sont les risques ?

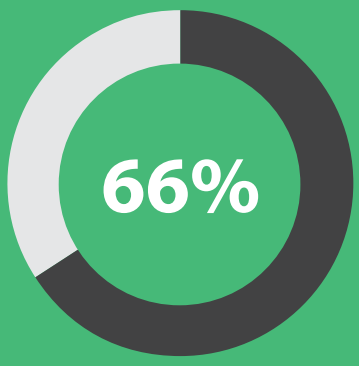
Par exemple, une erreur dans un algorithme qui détermine la solvabilité d'un emprunteur, même si un infime pourcentage seulement des demandes est mal calculé, peut avoir des conséquences catastrophiques à long terme sur la qualité du portefeuille de prêts de la banque lorsqu'elle s'applique à des milliers, voire des millions de prêts.

Les systèmes d'automatisation des processus robotisés et d'intelligence artificielle sont programmés par l'homme. Ils traitent des données elles aussi sélectionnées et affinées par des personnes, ce qui peut être source d'erreurs. Les institutions financières courent donc le risque de voir leurs algorithmes involontairement proposer des décisions biaisées à grande échelle ou être discriminatoires à l'égard de certains groupes démographiques. Elles en seraient alors tenues pour responsables, même si la discrimination n'est pas intentionnelle. Dans le cas de la souscription à des produits financiers, il est essentiel d'adopter une approche fondée sur les risques précise et capable de traiter objectivement et équitablement les clients. Le RGPD reconnaît cette problématique et exige que les personnes concernées se voient proposer des moyens simples de demander une intervention humaine ou de contester une décision fondée sur un processus automatisé. De plus, des vérifications doivent régulièrement être effectuées afin de s'assurer que les systèmes fonctionnent comme prévu.



36 % des responsables de l'audit interne déclarent que la digitalisation est un des cinq principaux risques auxquels leurs organisations sont confrontées

Source : Sondage réalisé auprès de nos membres

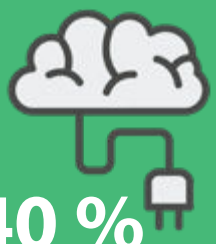


66 % des responsables de l'audit interne déclarent que les risques liés à la digitalisation et à l'adoption des nouvelles technologies constitueront un aspect important de leur travail en 2019 et dans les années à venir

Source : Entretiens réalisés auprès de nos membres

« L'**automatisation**, la robotisation, l'IA, tout cela génère beaucoup **d'incertitude** pour les organisations. Si des travaux doivent être effectués par des robots, cela affecte le **comportement** des collaborateurs. Quels sont ces comportements ? Quelle est leur influence sur la **culture** de l'entreprise ? Est-ce qu'ils ignorent ces évolutions, parce qu'ils en ont peur ? Il y a un **facteur humain** très important dans les risques liés aux systèmes d'information. Les gens qui se sentent en insécurité se comportent d'une manière spécifique. Les risques encourus par les organisations sont donc encore **plus importants** lorsqu'elles décident de nouvelles activités, surtout dans des domaines qu'elles **maîtrisent moins** ».

Responsable de l'audit interne, cabinet de prestations externes, Pays-Bas



40 %

Plus de 40 % des managers opérationnels prévoient que l'IA commencera à remplacer certains employés dans leur secteur d'ici 2021

Source : Economist Intelligence Unit

« Nous sommes **assez agiles face à l'innovation**. Nous avons commencé à utiliser l'intelligence artificielle, la robotique, l'analyse de données et d'autres interfaces numériques. Toutefois, nous comprenons moins les **risques associés** à ces innovations et où nous nous laissons entraîner. Quels sont les risques liés à l'intelligence artificielle, à la robotique et à la digitalisation des organisations ? Ils ne sont **pas toujours bien compris** ».

Responsable de l'audit interne, établissement financier, Royaume-Uni

Le déploiement des technologies a également des conséquences sur la culture de l'organisation. En effet, il peut susciter une certaine résistance liée à des incertitudes. Des reconversions ou des licenciements massifs sont à prévoir dans certains secteurs. Il est donc essentiel de comprendre l'impact que de telles initiatives peuvent avoir sur l'état d'esprit et le comportement des collaborateurs. Manifeste ou voilée, cette résistance doit être reconnue et gérée en conséquence dans la mesure où elle risque d'entraver l'introduction de nouvelles technologies.

Il est également important de rappeler que, pour l'instant, les technologies ne sont généralement qu'un outil complémentaire. En effet, il s'agit plus de travailler avec les technologies et de les utiliser pour accroître la productivité que d'être entièrement remplacés. Les entreprises qui laissent trop le contrôle à la technologie peuvent se trouver plus exposées aux risques. De plus, il est nécessaire de comprendre la manière dont les employés pourront interagir et utiliser des technologies telles que l'automatisation et l'intelligence artificielle afin d'optimiser leurs retombées positives et leur efficacité.

Les transformations à grande échelle requièrent l'adhésion et le soutien des principales parties prenantes, surtout de la part des cadres intermédiaires. Il n'est pas suffisant qu'un CTO (*Chief Technology Officer* ou responsable des infrastructures informatiques) supervise. Sans cette adhésion de tous les niveaux de management, les projets risquent de ne pas avoir l'élan nécessaire pour être mis en œuvre et être réalisés avec succès.

Tout projet technologique, qu'il s'agisse de la mise à niveau des systèmes ERP et CRM, du lancement de nouvelles applications, de l'intégration de fonctionnalités mobiles pour les clients ou du développement de systèmes d'automation ou d'intelligence artificielle, occasionnera des perturbations et d'éventuels problèmes de continuité d'activité, surtout lors de la phase de déploiement. Mais, il est primordial de faire en sorte que cette perturbation soit minime et d'assurer une transition sans heurts ou aussi harmonieuse que possible.

Du point de vue de l'audit interne

La direction générale et le conseil devraient avoir conscience des risques associés à l'adoption de nouvelles technologies. Il est probable que les promoteurs de ces technologies aient un solide *business case* en faveur de la digitalisation sans totalement en saisir les implications potentielles, et la deuxième ligne de maîtrise devrait s'efforcer d'identifier, d'évaluer et de communiquer ces risques à la direction générale et au conseil (l'absence d'analyse coûts/bénéfices, des bêta tests insuffisants, des erreurs d'algorithmes ou d'origine humaine, une résistance des collaborateurs ou des changements organisationnels par exemple). L'audit interne devrait rechercher des preuves de l'identification de ces risques, de la mise en place de plans pour les gérer, et signaler toute faiblesse potentielle dans le référentiel de maîtrise des risques.

Les projets ambitieux, comme l'utilisation de l'IA à grande échelle, peuvent exposer l'organisation à des risques excessifs surpassant les avantages qui pourraient en être tirés. C'est pour cette raison que les projets pilotes et une approche étape par étape sont généralement appropriés et proportionnés aux risques. Une fois que ces projets ont fait leurs preuves et ont été bien intégrés, l'organisation peut intensifier l'introduction de cette technologie. Il peut également être utile que l'organisation évalue la manière dont ses concurrents directs adoptent de nouvelles technologies, dans quelle mesure et pourquoi ils ont réussi, et si le marché a réagi positivement à de tels changements.

L'adoption de technologies devrait avoir pour but d'aider l'organisation à atteindre ses objectifs, et l'audit interne se doit donc d'évaluer si les projets sont en phase avec la stratégie. Ceci devrait être documenté et précisé de manière concrète et pas simplement conceptuelle. Ces précisions devront porter sur les processus concernés, les modalités de leur amélioration, et les indicateurs clés de performance qui permettront d'évaluer la technologie en question une fois qu'elle est opérationnelle, mais également ceux qui permettront de signaler l'inefficacité avérée ou potentielle des principaux dispositifs de contrôle. L'audit interne devrait avoir des objectifs et des approches clairement formulés en précisant la manière dont les processus seront affectés, et ce que cela implique en matière de risques et de systèmes de contrôle. L'audit interne a également un rôle d'assurance à jouer dans la vérification que les technologies fonctionnent comme prévu. Cela peut nécessiter de tester l'exactitude des données d'entrée, les algorithmes qui traitent ces données ainsi que la cohérence et la reproductibilité des résultats. L'audit interne devrait donc commencer par déterminer s'il possède les compétences nécessaires pour évaluer la technologie en question.

Questions clés

- Quelles sont les différentes technologies adoptées ? Existe-t-il une justification claire et documentée à cette introduction ? Est-elle compatible avec les objectifs opérationnels et stratégiques de l'organisation ?
- Qui sont les responsables de ces projets ? Prennent-ils en compte les risques potentiels associés à la digitalisation ?
- Dans quelle mesure les nouvelles technologies nécessiteront-elles des mises à jour et des modifications de l'environnement de contrôle ? La première ligne de maîtrise des risques est-elle chargée de mettre en œuvre ces modifications ?
- L'adhésion et le soutien du management intermédiaire sont-ils suffisants pour susciter l'élan nécessaire à la réussite de l'adoption de la technologie ?
- Les collaborateurs sont-ils réticents à ces projets, ont-ils un impact négatif sur la culture de l'organisation ? Le cas échéant, quelles étapes peuvent être mises en place pour mesurer cet impact et y remédier ?
- Les processus automatisés font-ils l'objet d'une évaluation en termes de qualité des données, d'exactitude des algorithmes et des résultats obtenus, et la fonction d'audit interne possède-t-elle les compétences qui lui permettront de confirmer que les technologies fonctionnent comme prévu ? Dans le cas contraire, qui fournit une assurance indépendante dans ce domaine ?

« C'est un **immense défi** pour l'audit interne, car si nous avons assisté à un **virage technologique** ces dix dernières années, l'audit interne n'a pas encore effectué le sien. Généralement, les auditeurs internes aiment les thèmes **concrets,** or la transition est **de plus en plus rapide**. Il n'est pas nécessaire d'avoir des **compétences** dans les domaines de l'automatisation ou de l'intelligence artificielle, mais vous devez comprendre et évaluer le *business case* et **la gestion de projet**. Les ressources du projet sont-elles suffisantes pour répondre aux attentes ? Les risques ont-ils été analysés par la direction générale en fonction des objectifs ? Vous pouvez effectuer un **audit traditionnel** même lorsque vous traitez d'évolutions technologiques **de pointe** ».

Responsable de l'audit interne,
cabinet de prestations externes, Suède

15 %

Actuellement,
15 % seulement des entreprises utilisent l'intelligence artificielle...

31%

... mais ce chiffre devrait atteindre les 31 % dans les 12 mois à venir

Source : Adobe

87%

87 % des entreprises industrielles prévoient d'introduire l'intelligence artificielle dans leur chaîne de production au cours des trois prochaines années...

...mais **28%** seulement ont établi un plan de mise en œuvre exhaustif

Source : Boston Consulting Group

« Nous avons moins de projets en termes de volume, mais ceux dont nous nous chargeons **sont axés sur la digitalisation.** Nous devons effectuer un virage technologique, ce qui signifie moins de projets avec des **budgets plus importants,** et implique une mise à niveau de l'infrastructure informatique ainsi qu'une numérisation des systèmes de back-office. En termes de **protection des actifs,** la bataille se joue sur l'audit de ces projets continus. En effet, il sera plus difficile de vérifier un projet déjà finalisé et de le modifier après coup. C'est une **perte de temps** et d'argent. L'audit interne doit être présent au cours du projet pour donner l'assurance au Conseil et au directeur général que la méthode de **conduite de projets** est bien respectée ».

Responsable de l'audit interne, compagnie d'assurance, Suède

DÉVELOPPEMENT DURABLE : ÉTHIQUE ENVIRONNEMENTALE ET SOCIALE

Les législateurs et l'opinion publique sont de plus en plus exigeants et attendent une responsabilité sociale et environnementale de la part des entreprises. Ainsi, le reporting en matière de développement durable devient un véritable enjeu et les décisions stratégiques des entreprises pour leur croissance à long terme intègrent cette responsabilité.

27 % des personnes interviewées citent l'éthique environnementale et sociale parmi les points à surveiller ; c'est la première année que ce thème figure dans le rapport « Risk in focus ». Cette tendance est particulièrement flagrante aux Pays-Bas où la moitié des responsables de l'audit interne soulignent que ce domaine nécessite une attention particulière. Toutefois, seuls 8% des répondants au sondage ont identifié l'environnement et les changements climatiques parmi les cinq risques les plus importants pour leur organisation.

La directive européenne sur le reporting extra-financier, en vigueur depuis 2017, exige que les entreprises cotées et les banques de plus de 500 employés publient des rapports concernant les politiques mises en place, les risques pertinents et les performances. Voici les politiques concernées :

- Protection de l'environnement
- Responsabilité sociale et traitement des collaborateurs
- Respect des droits de l'homme
- Lutte contre la corruption
- Diversité au sein des conseils de l'entreprise

Ces nouvelles exigences sont perçues comme une avancée ; elles favorisent la transparence et soulignent les efforts entrepris par les organisations pour atteindre leurs objectifs environnementaux et sociaux. Cependant, un des défis majeurs concerne l'exactitude des informations. Ce type de reporting est bien moins mature que le reporting financier, et les entreprises n'ont pas toutes les ressources nécessaires pour mesurer et analyser les indicateurs clés de performance. Elles risquent ainsi d'accroître leur risque de réputation si leurs activités étaient jugées contraires ou éloignées de leurs engagements. De plus, même lorsque le reporting extra-financier est suffisamment précis, tout indicateur clé de performance pouvant signifier que les pratiques de l'entreprise sont inférieures à celles de ses pairs pourrait être mal interprété par les investisseurs, qui font de plus en plus appel à des études comparatives afin de juger les performances en matière de gouvernance sociale et environnementale (ESG-*Environnemental and social governance).*

Il y a par ailleurs un risque stratégique lié au renforcement de la réglementation environnementale. La législation européenne est très étendue, de l'efficience énergétique des appareils électroménagers à la qualité de l'eau. Actuellement, les politiques les plus ambitieuses découlent de l'accord de Paris sur le changement climatique, qui vise à maintenir le réchauffement mondial en dessous de 2°C par rapport aux niveaux de l'ère pré-industrielle, en réduisant les émissions de carbone et autres gaz à effet de serre.

L'UE s'est déjà fixée des objectifs en matière d'émissions pour 2030 dans le cadre du système de « répartition des efforts ». Les États membres ont leurs propres objectifs individuels et sont garants des politiques nationales et des mesures mises en place afin de limiter les émissions. La tendance générale est à l'adoption de pratiques agricoles plus respectueuses du climat, à l'amélioration des performances énergétiques des bâtiments, à l'utilisation accrue des sources d'énergie renouvelables et à la réduction des émissions des véhicules.

En outre, la TCFD *(Task force on climate-related financial disclosures),* groupe de travail créé à l'initiative du G20, incite les entreprises à intégrer la gestion de leurs risques financiers liés au changement climatique et à la réduction des émissions de gaz à effet de serre dans leur communication externe. Bien que cette communication ne soit pas obligatoire, elle permet de transmettre aux investisseurs les informations dont ils ont besoin pour évaluer l'impact du risque climatique sur leurs portefeuilles.

Certains secteurs, comme l'automobile et les industries pétrolières et gazières, subissent donc une pression énorme pour comprendre les conséquences de ce renforcement des règlementations et des objectifs en matière d'émissions de carbone sur leur organisation, le développement de leurs produits et leurs stratégies. Cette réflexion cerne également leurs sous-traitants. Par exemple, une entreprise de produits chimiques qui tire une part importante de ses revenus des matériaux utilisés pour le blindage des moteurs diesel court un risque stratégique accru si elle ne diversifie pas ses activités dans de nouveaux secteurs de croissance, comme les batteries rechargeables pour voitures électriques.

Impact social

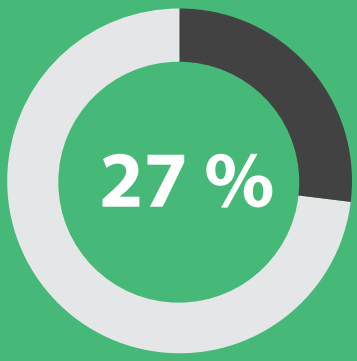
L'élan qui pousse les entreprises à se montrer de plus en plus socialement responsables et respectueuses des droits

Près d'un responsable de l'audit interne sur dix cite l'environnement et le changement climatique comme faisant partie des cinq risques principaux auxquels leur organisation doit faire face

Source : Sondage réalisé auprès de nos membres

« Une **discussion de fond** doit être engagée à propos du **rôle croissant** de la fonction d'audit interne en matière de développement durable. Maintenant que le **reporting extra-financier** est **obligatoire** pour les entreprises cotées, quel est notre rôle ? Sommes-nous tous supposés devenir des experts des émissions de carbone directes et indirectes ***(scope 1, 2 et 3)*** et de tous les autres sujets ? C'est une vraie question pour la profession d'audit ».

Responsable de l'audit interne,
groupe de distribution, Italie



27 % des responsables d'audit indiquent que les enjeux liés au développement durable constituent un domaine à cibler dans les années à venir

Source : Entretiens réalisés auprès de nos membres

40 %

Le cadre européen pour le climat et l'énergie fixe l'objectif de réduire d'au moins 40 % les émissions de gaz à effet de serre de l'Union Européenne d'ici à 2030, par rapport aux niveaux de 1990. Un certain nombre de pays, dont l'Allemagne, les Pays-Bas et le Royaume-Uni, se sont engagés à interdire la vente de nouvelles voitures essence et diesel à partir de 2030-2040.

Source : Commission européenne

« Nous fabriquons des produits pour le marché des véhicules diesel, les problématiques de **qualité de l'air** et de développement durable ont donc **particulièrement touché** notre entreprise, même si, au fil du temps, l'organisation s'est engagée dans le développement de **nouveaux matériaux**. Vous avez un **aspect législatif**, l'éthique et la conformité, mais il y a aussi les tendances du marché. Que se passe-t-il dans le monde qui puisse influencer notre **stratégie** et entraîner des changements stratégiques ? De ce fait, l'audit interne s'intéresse au processus de **planification stratégique** à sa pertinence et à sa **dynamique**, car l'environnement externe subit un grand nombre de modifications ».

Responsable de l'audit interne,
groupe chimique multinational, Royaume-Uni

2 000 milliards

L'effet du réchauffement climatique sur la productivité des travailleurs pourrait coûter plus de 2 000 milliards de dollars à l'économie mondiale d'ici 2030

Source : Recherche universitaire

de l'homme est un autre de leurs défis. Des rapports extra-financiers annuels sont devenus obligatoires pour expliquer les processus d'identification et de gestion des risques de violation des droits de l'homme.

Ayant adopté le *Modern Slavery Act* (loi contre l'esclavage moderne) il y a deux ans, les Britanniques ont déjà eu l'occasion de se familiariser avec cette problématique. De même, l'an dernier, l'Espagne a engagé son plan d'action national sur les droits de l'homme, à l'instar de l'Italie qui s'était déjà engagée dans cette démarche l'année précédente. Ces mesures mettent l'accent sur le besoin de respecter une intégrité éthique dans les opérations et chaînes d'approvisionnement en appliquant les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme.

Il convient toutefois de noter que si ces instruments contribuent à améliorer la transparence, il n'existe pas d'obligation légale contraignant les organisations à améliorer la diligence raisonnable ou à éradiquer les violations des droits de l'homme. En effet, elles ne sont astreintes qu'à la rédaction d'un rapport sur les mesures prises pour atténuer les risques éventuellement identifiés.

La loi sur le devoir de vigilance récemment entrée en vigueur en France va encore plus loin. À partir de 2018, les grandes entreprises françaises (de plus de 5 000 employés, ou 10 000 si le siège de la société ne se trouve pas en France) doivent publier un plan de vigilance qui a pour but de prévenir les risques liés à l'environnement, aux droits de l'homme et à la corruption, non seulement en ce qui concerne leurs propres activités, mais également celles de leurs filiales, sous-traitants et fournisseurs. De plus, si ces plans ne sont pas correctement mis en œuvre, les entreprises pourront faire l'objet de poursuites civiles.

Si cette loi se montre efficace, il est fort probable que d'autres pays, particulièrement en Europe, introduisent une législation avec les mêmes pouvoirs de sanction. Même si ce n'est pas le cas et que l'éthique sociale continue à se limiter à une obligation de reporting, il n'en demeure pas moins que l'opinion publique exige aujourd'hui que les entreprises endossent la responsabilité des conséquences sociales et environnementales de leurs activités. Face à ces risques de réputation, toute transgression peut être source de dommages durables pour les marques et le cours des actions.

Du point de vue de l'audit interne

Les organisations doivent dorénavant rendre compte des mesures mises en place afin d'identifier et de réduire les risques en matière de développement durable. Pour ce faire, elles peuvent se référer à des normes comme celles du GRI *(Global Reporting Initiative)*. Plusieurs Instituts ont également produit des guides dans ce domaine comme les travaux du Chartered Institute of Internal Auditors du Royaume-Uni sur les rapports extra-financiers : bit.ly/IIAnon-fin

La fonction d'audit interne peut contribuer à ces initiatives en s'assurant simplement que les exigences en matière de reporting sont respectées. Elle peut toutefois aller plus loin en prouvant que les déclarations faites dans les rapports extra-financiers sont exactes, exhaustives, à jour et effectives. Il est également utile de recueillir des données quant à la manière dont des processus sont développés afin d'améliorer ce reporting, comme le nombre d'indicateurs clés de performance mesurés et l'exactitude des données collectées. Les missions d'audit les plus approfondies peuvent évaluer les rapports de développement durable dans l'ensemble du secteur concerné afin de comparer le reporting et les performances de l'organisation à ceux de ses pairs.

Les obligations en matière de respect des droits de l'homme par les entreprises sont relativement récentes et restent très générales, et elles sont souvent centrées autour des travaux de reporting qui sont menés afin de minimiser les dommages corporels. Cependant, les lois environnementales sont déjà bien développées en Europe et, au besoin, les programmes d'audit de conformité peuvent inclure l'assurance que la législation sectorielle en matière d'environnement est respectée. En dépit de leur conformité réglementaire et juridique, de nombreuses organisations font face à une menace fondamentale liée aux objectifs en matière d'émissions de carbone, et la fonction d'audit interne peut être tenue de fournir l'assurance que la direction générale en tient compte dans le cadre de ses prises de décision stratégiques.

Il est important de ne pas négliger les dommages que des incidents liés aux droits de l'homme et à l'environnement peuvent causer à une organisation. Respecter des exigences légales et des règles ne remplace pas une amélioration constante au regard des normes ESG, et la fonction d'audit interne peut régulièrement offrir un point de vue indépendant sur les progrès réalisés dans le but d'améliorer les opérations et de limiter, à moyen et long terme, les dommages sociaux et environnementaux.

Questions clés

- L'organisation publie-t-elle des rapports extra-financiers comme l'exige la législation européenne ?
- L'audit interne a-t-il la possibilité d'évaluer la maturité du reporting exta-financier et d'examiner dans quelle mesure les déclarations de l'entreprise en matière d'éthique environnementale et sociale reflètent la réalité ?
- L'organisation évalue-t-elle la performance en matière de développement durable à la lumière des indicateurs clés de performance du secteur ? Y a-t-il un écart entre l'entreprise et ses pairs concernant les pratiques de reporting et les performances extra-financière ?
- L'organisation respecte-t-elle toutes les lois environnementales pertinentes, dans tous les territoires ?
- Dans quelle mesure le renforcement de la réglementation environnementale est-il susceptible d'influer sur la stratégie de l'entreprise (sur les objectifs de réduction des émissions de carbone par exemple) ? La direction générale est-elle informée de cet impact potentiel ?
- La direction générale saisit-elle l'importance d'améliorer continuellement les opérations afin de réduire les dommages environnementaux et sociaux ?
- Quelle est la valeur ajoutée de l'audit interne lorsqu'il évalue et confirme de manière étayée les améliorations pertinentes en matière de développement durable ?

Environ la moitié des États membres de l'Union Européenne n'ont pas respecté l'échéance de décembre 2016 pour la transposition de la Directive sur le reporting extra-financier dans leur législation nationale. En décembre 2017, tous les États avaient adapté leur législation afin de prendre en compte les obligations de la directive. Cela signifie que nous ne commencerons à avoir une idée claire de la conformité et de la qualité du reporting de développement durable qu'à partir de 2019.

22 % des entreprises dans le monde s'attaquent aux problèmes liés au travail des enfants dans la chaîne d'approvisionnement...

...**23 %** luttent activement contre le dérèglement climatique...

... et **32%** seulement assurent ne pas s'approvisionner dans des zones touchées par des conflits et autres situations de violence

Source : Economist Intelligence Unit

« Nous sommes en train d'être évalués par l'indice Dow Jones de développement durable. Ce sont les **marchés financiers** qui nous y poussent, car certains fonds **n'investissent** que dans le cadre d'un programme de développement durable. Nous respectons également des **lois environnementales.** Si vous investissez dans le secteur alimentaire, vous devez reconnaître que les ressources sont limitées et qu'il est essentiel de se montrer **responsable** envers la planète et les animaux. Il est important pour nos clients que nos produits proviennent de **ressources durables,** nous devons donc vérifier que c'est bien le cas ».

Responsable de l'audit interne, groupe de distribution, Allemagne

« C'est plutôt rare, mais ma fonction d'audit interne s'occupe également de la **responsabilité sociale de l'entreprise**, je coordonne donc le processus de développement durable ainsi que le reporting, qui sont tous deux **obligatoires** à partir de cette année pour les entreprises cotées. Je suis aussi chargé de soutenir l'activité en **suivant** les **progrès** effectués au regard des objectifs et du référentiel de développement durable. Les risques de développement durable sont donc importants pour moi et ils ont largement été pris en compte pour le plan d'audit de **l'année prochaine**. Avec une équipe différente, je commence à fournir une assurance dans ce domaine. Nous ne nous intéressons pas uniquement aux **indicateurs clés de performance** internes en matière d'environnement, de **droits de l'homme**, de diversité et d'inclusion, mais également à toute la chaîne d'approvisionnement. »

Responsable de l'audit interne, groupe de distribution, Italie

CONFORMITÉ ANTI-CORRUPTION

Les risques de corruption sont anciens. Toutefois, les réformes locales, leur mise en oeuvre coordonnée à l'échelle mondiale par les organismes de contrôle et les amendes sans précédent augmentent les enjeux et propulsent cette problématique au premier rang des priorités.

Nous avons découvert qu'une personne sur cinq interrogée dans le cadre de nos entretiens mentionnait les risques liés au programme de conformité anti-corruption et la nécessité de l'intégrer au programme d'audit en 2019. La moitié des responsables d'audit s'intéressant à cette question étaient en Espagne. Tous les secteurs étaient concernés, à l'exception de la distribution et de l'information/technologie/communication. Par ailleurs, selon le sondage, 58% des répondants considèrent la conformité comme un des cinq risques les plus importants, juste derrière la cybersécurité (66%) et à égalité avec la sécurité des données.

Ces constats coïncident avec l'effort récent d'un certain nombre de pays pour réformer ou entamer un processus de modernisation de leurs lois anti-corruption. De manière générale, ces réformes sont similaires à la loi anti-corruption *(Bribery Act)* du Royaume-Uni qui interdit la corruption privé-public et privé-privé ainsi que l'implication d'agents et autres tiers.

- La Chine a mis à jour sa loi contre la concurrence déloyale début 2018, élargissant la responsabilité aux tentatives de corruption effectuées par des tiers.

- L'Irlande a mis à jour sa loi anti-corruption en 2018 pour y introduire un certain nombre de nouvelles infractions et a élargi leur champ d'application au-delà de la corruption des agents publics pour y inclure les entreprises privées.

- Le gouvernement australien a une série de projets de loi couvrant la corruption internationale, y compris le nouveau délit de « défaut de prévention de la corruption d'un agent étranger » dans la ligne du *Bribery Act* au Royaume-Uni.

- La France a adopté une nouvelle loi sur la transparence et la lutte contre la corruption (loi Sapin II) qui peut engager la responsabilité des entreprises qui n'auraient pas mis en place un programme anti-corruption efficace, et ce qu'il y ait eu corruption ou non.

L'Agence française anti-corruption créée dans le cadre de cette Loi Sapin II a publié des recommandations en décembre 2017 qui sont graduellement mises en œuvre depuis début 2018.

Une mise en oeuvre coordonnée

En plus du renforcement de la législation, tendance qui devrait se poursuivre, il existe des éléments probants de la coordination des travaux et du partage des informations entre les agences anti-corruption pour sanctionner les contrevenants, et ce dans plusieurs juridictions. En 2016, 42 % des décisions en matière de corruption étrangère aux États-Unis ont impliqué une coopération avec des autorités d'autres pays, une augmentation significative par rapport à la décennie précédente [6]. Cette collaboration a pour conséquence d'accroître les risques d'infraction.

Cette coopération été mise en évidence lors de la plus grande affaire de corruption jamais mise au jour. En décembre 2016, la société d'ingénierie et de construction brésilienne Odebrecht a accepté de payer une amende record s'élevant à 3,5 milliards de dollars après avoir été accusée d'avoir soudoyé, à hauteur de plusieurs milliards de dollars, des responsables de la compagnie pétrolière Petrobras. Des amendes ont notamment été payées aux autorités brésiliennes, suisses et nord-américaines.

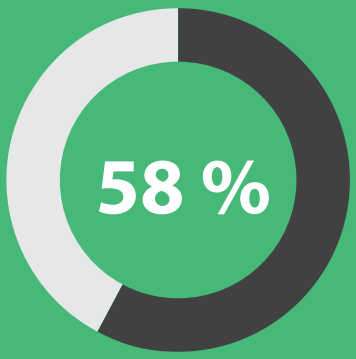
Finalement, l'amende a été réduite à 2,6 milliards de dollars. Néanmoins, la société a perdu d'importants projets de construction initialement prévus avec les gouvernements du Pérou, de Colombie et du Panama. Ces événements montrent clairement que les conséquences financières de la violation des règles anti-corruption s'étendent bien au-delà des amendes financières ; elles peuvent être particulièrement critiques sur le plan commercial.

Programme anti-corruption

Pour éviter de lourdes amendes, les organisations devraient développer et mettre en place un programme anti-corruption qui leur permette de démontrer leurs valeurs éthiques et leur engagement dans la lutte contre la corruption. L'organisation devrait ainsi montrer clairement que la corruption, sous toutes ses formes, directe ou indirecte, est interdite (« tolérance zéro »). La mise en place d'un tel programme montre également que l'organisation déploie des efforts raisonnables pour s'assurer que des pots-de-vin ne sont ni versés ni reçus. Il devrait tenir compte de toutes les lois et réglementations pertinentes ainsi que des instructions particulières qui s'appliquent dans les pays dans lesquels l'entreprise opère. Ce programme devrait être proportionné, tenir compte des risques de corruption propres au secteur concerné, de la taille de l'organisation et de la complexité de ses activités, aussi bien que des différents territoires dans lesquels elle opère. Cela permettra de réduire considérablement les risques de lourdes amendes en cas de non-conformité.

Un responsable de l'audit interne sur cinq affirme que les programmes de conformité anti-corruption seront une priorité pour 2019

Source : Entretiens réalisés auprès de nos membres

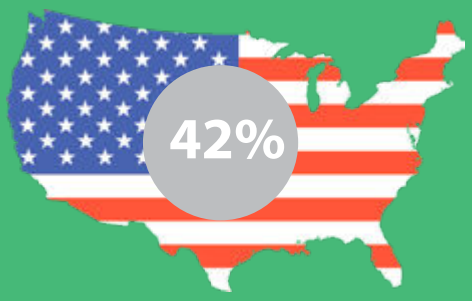


58 % des responsables d'audit ont placé la conformité parmi les cinq principaux risques, juste après la cybersécurité ; 13 % affirment qu'il s'agit du risque le plus important auquel leur organisation est confrontée

Source : Sondage réalisé auprès de nos membres

« Les réglementations **anti-corruption**, montrent à quel point il serait **idiot** de penser uniquement à générer d'énormes profits pour devoir ensuite payer des amendes, simplement parce que vous n'avez pas **respecté avec suffisamment de rigueur** les recommandations de l'Agence française de lutte contre la corruption ou, pire encore, pour avoir violer le ***Foreign Corrupt Practices Act*** américain. Il faudrait alors **payer une amende considérable** et être suivi par le ministère de la Justice pendant trois ans. C'est pour cela que les audits de conformité sont si importants ».

Responsable de l'audit interne, entreprise multinationale d'ingénierie, France



En 2016, 42 % des décisions en matière de corruption étrangère aux États-Unis ont impliqué une coopération avec des autorités d'autres pays

Source : ministère de la Justice, États-Unis

« Nous essayons d'établir les mêmes normes, politiques de risques et la même gouvernance dans l'ensemble du groupe. Nous nous intéressons toujours de près à la corruption et aux relations que nous entretenons avec les **tiers** auxquels nous **payons des licences** dans les pays où nous sommes en **pleine croissance et où nous construisons.**
L'effort d'investissement est important en **Amérique latine** et dans ces pays, la corruption avec les tiers est un enjeu de taille en termes de sanctions et de réputation ».

Responsable de l'audit interne,
groupe multinational de services publics, Espagne

1 500 milliards

On estime que la corruption coûte chaque année 1 500 milliards de dollars aux entreprises et particuliers. Cela représente environ 2 % du PIB mondial

Source : Banque mondiale

« La France a adopté une nouvelle loi dite « Sapin II », et il existe désormais une nouvelle agence de lutte contre la corruption qui vise les entités publiques comme les nôtres, mais également les entreprises privées. Les modalités d'application de la loi ayant été précisées fin 2017, cela constituera donc un enjeu de conformité majeur à partir de 2019. Et il en va de même pour la mise en œuvre et le suivi de la protection des données dans le cadre du RGPD. Il s'agit sans aucun doute des deux principaux enjeux de conformité auxquels nous sommes confrontés aujourd'hui, et la fonction d'audit interne devra s'y intéresser ».

Responsable de l'audit interne, secteur public, France

Un programme anti-corruption efficace démontre que l'organisation déploie des efforts raisonnables pour maîtriser les risques de conformité. Les autorités prendront cela en considération lors d'une enquête pour corruption. Il est donc dans l'intérêt de l'organisation de signaler elle-même aux autorités tout problème de corruption éventuel et de coopérer pleinement à l'enquête. Le cas échéant, cela permettra probablement de réduire les amendes encourues.

Une norme internationale

L'introduction de la norme ISO 37001, la première norme définissant des systèmes de management anti-corruption, en 2016, définit un certain nombre de mesures que les entreprises peuvent mettre en place pour prévenir et détecter la corruption. Microsoft, première organisation à avoir engagé un processus pour obtenir la certification ISO 37001, a affirmé que le patchwork d'exigences des différentes agences gouvernementales et les nombreuses réformes compliquaient les efforts de lutte contre la corruption et augmentaient donc les risques. La nouvelle norme ISO peut être un moyen de gérer ce problème en créant un langage commun et des spécifications claires afin que les organisations puissent établir, mettre en œuvre, maintenir et améliorer continuellement leurs systèmes de management anti-corruption. Les entreprises qui considèrent que la corruption représente un risque devraient donc s'intéresser à la norme ISO 37001, au moins comme un point de référence.

Du point de vue de l'audit interne

La fonction d'audit interne a un rôle essentiel à jouer dans l'évaluation des efforts mis en place pour maîtriser les risques de corruption. La première étape consistera à comprendre la tolérance de la direction générale et du conseil à ces risques au regard de leur probabilité. Tous les secteurs avec des contrats publics significatifs (« construction/infrastructures », « pétrole/gaz », « industrie minière et autres activités extractives ») sont considérés comme ayant des risques importants, tout comme les territoires fortement touchés par la corruption.

La fonction d'audit interne devrait évaluer l'exhaustivité de la conception du programme anti-corruption de l'entreprise. Elle devrait inclure les valeurs de l'organisation, l'affirmation d'une politique de tolérance zéro, les codes de conduite à destination des collaborateurs et des fournisseurs, une évaluation des risques de corruption ainsi que les politiques et procédures en place, y compris le dispositif d'alerte. L'évaluation devrait comprendre les risques liés aux pays, aux secteurs d'activité, aux transactions et aux partenariats. Toute lacune identifiée dans la conception du programme anti-corruption devrait être signalée au conseil. L'étape suivante consiste à évaluer l'efficacité de chacun des éléments du programme.

La mission d'audit interne devrait également souligner auprès de la direction générale l'importance de signaler les incidents et de coopérer avec les autorités afin d'éviter les poursuites pénales et de réduire, voire d'annuler complètement, les sanctions financières. L'institut d'audit interne des Pays-Bas a publié un rapport détaillé sur ce thème. Vous pourrez le trouver ici : bit.ly/IIA_ABC

Questions clés

- L'organisation a-t-elle un programme anti-corruption suffisamment exhaustif ? Est-il effectivement mis en place ?
- La direction générale a-t-elle déclaré une politique de tolérance zéro ?
- Existe-t-il des programmes de sensibilisation et de formation du personnel, et une procédure d'alerte a-t-elle été établie ?
- Une culture anti-corruption se diffuse-t-elle dans toute l'organisation ?
- Une évaluation des risques concernant l'exposition de l'organisation à la corruption a-t-elle été réalisée ?
- La deuxième ligne de maîtrise est-elle suffisamment fondée sur une approche par les risques et axée sur les territoires et les unités opérationnelles les plus exposés aux risques de corruption ?
- La direction générale a-t-elle considéré l'obtention d'une certification ISO 37001 ? Dans le cas contraire, à quel cadre de référence l'organisation se réfère-t-elle ?
- Existe-t-il une séparation des tâches concernant les paiements de facilitation à des agents publics et à des conseillers ?
- Existe-t-il des politiques de diligence raisonnable vis-à-vis des tiers, et ces politiques sont-elles respectées ?

Les quatre principaux secteurs dans lesquels la corruption est la plus répandue concentrent 59 % de ces actes

- Activités extractives/mines
- Construction
- Transport et entreposage
- Information et communication
- Autres

Source : OCDE

"Nous avons l'impression que la corruption diminue. Dans le même temps, les contribuables et la presse **tolèrent de moins en moins** ce qu'ils considèrent comme des **comportements inappropriés**, de sorte que de plus en plus de cas font surface. Cette situation rend notre tâche encore plus ardue, car les médias ne manquent pas de demander **"où était l'audit interne ?"** lorsque des incidents sont révélés. Aujourd'hui, avec les réseaux sociaux, le moindre signe de corruption est amplifié et se répand partout".

Responsable de l'audit interne, secteur public, Suède

« On considère largement que nous sommes chargés d'évaluer **le risque potentiel** de **corruption** des fonctionnaires. À mon avis, le niveau de fraude est très **faible** au sein de notre ministère si vous le comparez au reste du pays. Mais même si le niveau est faible, chaque cas de corruption touchant le ministère est un problème **sérieux** ».

Responsable de l'audit interne, secteur public , Espagne

La corruption augmente de **10 %** les frais généraux des activités internationales. Cette augmentation peut atteindre jusqu'à **25 %** pour les marchés publics dans les pays en voie de développement

Source : UNPRI (Principes pour l'investissement responsable des Nations Unies)

57 % des pots de vin sont versés en vue de remporter des marchés publics...

... et, en deuxième position, **12%** sont payés pour faciliter des procédures de dédouanement

Source : OCDE

RISQUES LIÉS À LA COMMUNICATION : PROTÉGER LA MARQUE ET LA RÉPUTATION

Les risques pouvant occasionner un préjudice sur la marque ou la réputation prennent de l'importance à mesure que des défaillances très médiatisées sont rendues publiques. Les organisations doivent être attentives à l'image qu'elles donnent.

Au cours de notre enquête qualitative, nous avons constaté qu'un peu moins d'un responsable d'audit sur cinq comptait s'intéresser aux risques de communication en 2019 et durant les années suivantes. Parmi cette minorité de répondants, tous n'avaient pas l'intention d'inclure une mission sur ce sujet dans leur plan d'audit pour les 12 mois à venir. Cependant, les problèmes de marque et de réputation étant de plus en plus fréquents, ils ont néanmoins déclaré que cette problématique devait être surveillée. Ce qui reflète la tendance à être plus attentif à l'image que l'organisation projette vers l'extérieur.

Les risques liés à la communication doivent être entendus comme la possibilité pour une organisation de porter atteinte, involontairement, à sa propre marque ou à sa réputation en raison de déclarations publiques. L'importance de construire et de protéger la marque et la réputation est largement acceptée. En effet, la réputation peut avoir un impact aussi bien immédiat qu'à long terme sur la performance globale d'une organisation dans la mesure où elle contribue à augmenter les ventes et à attirer les capitaux ainsi que les talents. Un certain nombre d'incidents peuvent entacher la réputation d'une organisation, qu'il s'agisse de corruption, de fuite de données ou d'un service client très médiocre, et la réponse apportée dans l'espace public est en mesure d'atténuer ou d'aggraver considérablement les dommages causés. De plus, une mauvaise stratégie de communication ou une campagne marketing mal conçue peuvent, en elles-mêmes, avoir un impact négatif sur la réputation de l'organisation.

De ce fait, les entreprises doivent prêter une attention particulière à l'image qu'elles renvoient ainsi qu'aux valeurs qu'elles portent sur la place publique. Ceci se révèle tout particulièrement vrai dans notre époque où les réseaux sociaux, instantanés et transparents, sont omniprésents et où un seul tweet peut rapidement avoir des conséquences imprévues. Par exemple, en 2017, McDonald's a publié un message anti-Trump/pro-Obama qui, malgré son retrait rapide, a été retweeté et « liké » plus d'un millier de fois. Peut-être un peu naïvement, l'entreprise n'avait semble-t-il pas prévu le retour de bâton des partisans de Donald Trump et le mouvement #BoycottMcDonalds qui a suivi. Elle a ensuite présenté ses excuses, expliquant que son compte avait été piraté.

Les plateformes de réseaux sociaux ont facilité un dialogue direct et spontané avec les clients tout en donnant une voix et une identité aux entreprises. Ces plateformes sont devenues des outils marketing low-cost et réactifs qui permettent d'attirer l'attention de millions de personnes. Mais les réseaux sociaux augmentent aussi les risques de réputation. À l'heure de la polarisation politique, les sensibilités sociales sont exacerbées et « dire ce qu'il ne faut pas » peut sérieusement nuire à l'identité de la marque. Les organisations doivent donc être particulièrement attentives aux messages envoyés sur les réseaux sociaux et dans le cadre de leurs stratégies marketing et de communication qui pourraient être jugés inappropriés.

Stratégie, politiques et responsabilités

L'élément clé du marketing est son efficacité. L'audit interne a un rôle à jouer lorsqu'il s'agit de prouver l'efficacité des budgets et dépenses de marketing, en particulier lorsque cet impact est quantifiable, comme les paiements par clic pour le marketing digital. Ces questions se limitent alors à l'efficience opérationnelle et ne traitent pas du risque de réputation. De même, il y a des considérations liées à la conformité de la commercialisation des produits et services, en évitant, par exemple, les déclarations et représentations trompeuses ou de cibler les enfants. Là encore, l'audit interne peut apporter une valeur ajoutée en s'assurant que des dispositifs de contrôle sont en place pour atténuer le risque de non-conformité par rapport aux réglementations en vigueur en matière de marketing, comme celles imposées par l'Ofcom au Royaume-Uni, ce qui pourrait nuire à la réputation de l'organisation.

Il faut toutefois considérer que même une campagne marketing entièrement conforme aux lois et règlements en vigueur, qu'elle soit développée sur les réseaux sociaux ou non, est susceptible de se révéler inappropriée ou de choquer le public, même involontairement. Ainsi, en 2018, l'enseigne de vêtements H&M a été publiquement condamnée pour avoir commercialisé un produit porté par un jeune garçon noir affichant le slogan *« Coolest monkey in the jungle »* (le singe le plus cool de la jungle). L'entreprise a ensuite présenté ses excuses à tous ceux qui auraient été offensés et a retiré la photo du site, mais l'incident a néanmoins suscité des protestations dans les magasins sud-africains de l'enseigne.

75 % des administrateurs considèrent les risques de réputation comme une préoccupation majeure...

...toutefois, **6 %** seulement affirment maîtriser les enjeux liés aux réseaux sociaux

Source : EisnerAmper

« Nous avons pu constater qu'un certain nombre d'organisations **échouent manifestement** à gérer leurs problèmes de communication. **Oxfam** est un bel exemple de ce qu'il ne faut pas faire quand on gère une crise. La réponse du directeur général a été épouvantable. Mais d'autres, comme **TSB** se sont montrés exemplaires en retirant leurs publicités et en **présentant leurs excuses** pour les erreurs qu'ils avaient commises. Les services de communication doivent savoir qui les **autorise à agir,** ils doivent connaître les régulateurs, les gouvernements, les principaux fournisseurs, bailleurs de fonds ou clients, et la manière d'interagir avec eux. Ces points d'attention sont particulièrement importants pour les **réseaux sociaux** et la façon dont l'organisation communique sur ces plateformes. Il faut avoir une **vision stratégique** de l'audience ».

Responsable de l'audit interne, secteur public, Royaume-Uni

LES 7 DIMENSIONS DE LA RÉPUTATION

Selon le *Reputation Institute*, la réputation a 7 dimensions qui influencent la manière dont l'entreprise est perçue :

Leadership
Comment votre entreprise mène-t-elle le jeu ? Les entreprises ayant à leur tête un directeur général et des cadres dirigeants qui prennent position sur les questions cruciales, souvent controversées, ont tendance à avoir plus de succès que les organisations plus discrètes.

Performance
Les chiffres comptent. La performance et la rentabilité sont des indicateurs clés d'une bonne réputation.

Produits
Délivrer continuellement des produits et des services de qualité détermine la valeur d'une entreprise.

Innovation
Votre entreprise est-elle statique ou dynamique ? Les organisations innovantes qui savent dépasser le statu quo avec créativité sont plus appréciées que les autres.

Environnement de travail
La culture d'entreprise a une incidence directe sur le recrutement, la fidélisation, la qualité, la capacité et la motivation des ressources humaines – un des actifs les plus importants de l'entreprise – pour mettre en œuvre la stratégie.

Gouvernance
Ce n'est qu'avec le soutien de ces parties prenantes que l'entreprise acquière le droit d'exercer et le bénéfice du doute dont découle une croissance soutenue.

Engagement citoyen
Comment votre entreprise apporte-t-elle de la valeur ajoutée au-delà des produits et services qu'elle propose ? La responsabilité sociale de l'entreprise, les dons de bienfaisance, le bénévolat et les campagnes philanthropiques contribuent à rendre le monde meilleur.

Pour s'assurer que « le message à passer » est bien respecté, l'organisation doit élaborer une stratégie pour guider la manière dont elle se présente au public. Cette stratégie devrait être en phase avec les valeurs et l'identité de la marque, et être cohérente sur tous les réseaux. Tous les collaborateurs des services marketing et de communication devraient connaître et avoir accès à des instructions formalisées ainsi qu'à des politiques encadrant ce qui peut être dit ou non. Cela se révèle particulièrement important pour les réseaux sociaux, qui sont souvent considérés en complément des stratégies de communication existantes. En effet, les réseaux sociaux ne devraient pas être une fin en soi, mais liés à des objectifs plus larges de l'organisation.

Des processus d'approbation appropriés, en fonction des supports de communication, devraient également être mis en place afin d'atténuer les risques de réputation. Par exemple, les communiqués de presse programmés sont susceptibles d'être approuvés par le responsable des relations publiques/communication, tandis qu'un responsable du marketing pourra signer des tweets et autres messages destinés aux réseaux sociaux. L'objectif est de générer une gouvernance forte, un management hiérarchique efficace et un devoir de rendre compte, qui devront tous être formalisés et communiqués aux collaborateurs concernés.

Maîtrise des préjudices

Un plan de gestion de crise devrait également être mis en place dans l'éventualité d'une situation délicate, que ce soit en lien avec les activités courantes de l'organisation, des commentaires de son directeur général ou de ses dirigeants, ou d'une mauvaise campagne marketing. Il est également conseillé que les membres de la direction générale soient sensibilisés aux relations avec la presse. En effet, le public attendra une réponse rapide et appropriée, et l'organisation devrait savoir faire amende honorable et « assumer » publiquement ses erreurs de jugement. Dans ce domaine, le ton compte. Les messages devront être sincères et empathiques, et ne pas chercher à exonérer l'organisation (voir le commentaire de Oxfam sur la page ci-contre). Il est peu probable que les discours prêts à l'emploi soient accueillis favorablement, et une solution devrait être proposée (analyse du problème afin qu'il ne se reproduise plus, retrait des propos incriminés, par exemple). Dans de nombreux cas, une réponse rapide, appropriée, mesurée et authentique sera suffisante pour atténuer ce qui aurait pu se transformer en une situation catastrophique capable de porter préjudice à la réputation de l'organisation.

Du point de vue de l'audit interne

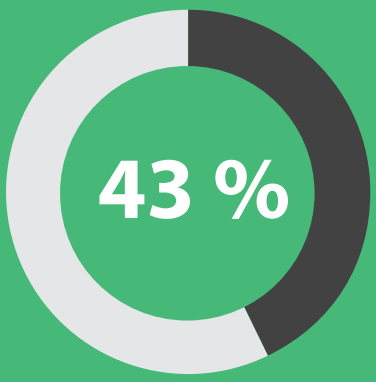
La direction générale et le conseil devraient reconnaître la valeur de la marque et être conscients qu'une réputation prend des années à se construire, mais qu'il ne faut que quelques minutes pour la ternir. Si l'organisation souhaite avoir une assurance concernant les risques liés à la communication, l'audit interne devrait s'intéresser à la définition claire des rôles, des responsabilités, de l'attribution des messages et du devoir de rendre compte. Les processus d'approbation permettent de s'assurer que les communications ont été vérifiées et que tout message potentiellement choquant ou ambigu ne sera pas publié. Les risques peuvent aussi être atténués grâce à des règles et à des politiques de communication correctement formalisées qui précisent ce qui peut être dit ou les thèmes à éviter. Parmi les autres dispositifs de contrôle interne et processus, on peut citer la gestion des droits d'accès, qui permettent de s'assurer que seules les personnes disposant de l'autorité nécessaire peuvent publier sur les réseaux sociaux et blogs de l'entreprise, ainsi que les plans de gestion de crise, qui aideront l'organisation à réagir si des actes répréhensibles la concernant sont rendus publics ou que des communications (comme des campagnes marketing ou des publications sur les réseaux sociaux) sont mal reçues.

« J'ai prévu une mission d'audit en 2019 sur les réseaux sociaux. Je veux m'assurer que les risques associés à cette stratégie de communication sont faibles et que nous mettons en place des dispositifs de contrôle solides pour surveiller la manière dont l'entreprise gère ses comptes de réseaux sociaux. Cette ressource importante pour le marketing et la communication se gère à l'échelle de l'organisation. Nous disposons également de canaux pour notre directeur général, qui est très médiatisé, et d'autres canaux pour chacune de nos marques. C'est clairement un risque à cibler pour nous ».

Responsable de l'audit interne, groupe de distribution, Italie

Questions clés

- Le conseil et la direction générale sont-ils conscients qu'une mauvaise communication peut nuire à la réputation de l'organisation ?
- Qui est responsable des différents moyens de communication de l'organisation et ces personnes ont-elles conscience de leur devoir de rendre compte ?
- Les collaborateurs chargés du marketing connaissent les grandes lignes de la marque : son identité, les thèmes à aborder ou à éviter (par exemple, les règles relatives à l'engagement dans les débats politiques) ?
- Les politiques encadrant ce qui peut être dit ou non, et la séparation des rôles et des responsabilités sont-elles correctement formalisées ?
- Les droits d'accès, tels que la modification des comptes de réseaux sociaux et des mots de passe lorsque des collaborateurs quittent l'entreprise, sont-ils correctement gérés ?
- Un plan de gestion de crise incluant la direction générale et la fonction de communication a-t-il été mis en place ?
- L'organisation utilise-t-elle des scénarios de communication et tire-t-elle des leçons des erreurs commises par ses concurrents ?
- L'organisation organise-t-elle des formations à destination des collaborateurs qui interagissent avec les médias (Directeur général, Président, par exemple) ?



43 % des dirigeants d'entreprise à travers le monde considèrent que leur organisation est très sensible aux risques de réputation

Source : British Standards Institution

« Il existe un **risque réel** que la réputation d'une organisation soit entachée si elle ne considère pas les questions d'éthique comme il se doit et si elle est incapable de gérer correctement sa relation aux médias. La **gestion des médias** est cruciale. Nous communiquons beaucoup, de plus en plus via les **réseaux sociaux**, et nous devons être conscients de la façon dont l'organisation est **perçue** ».

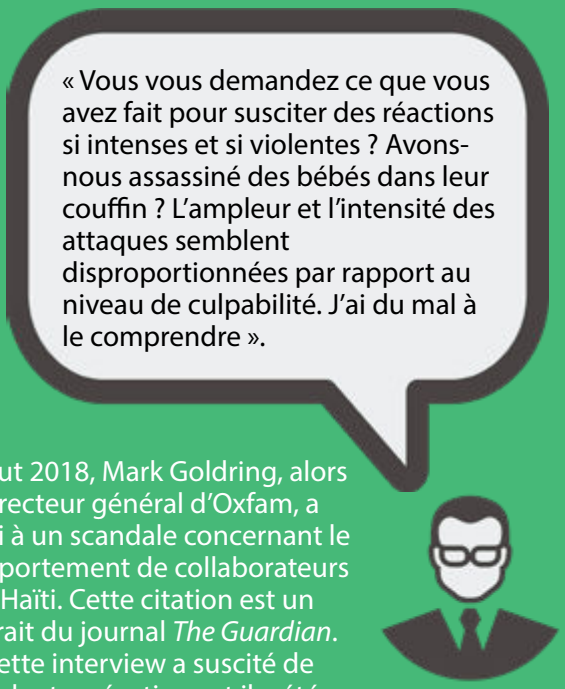
Responsable de l'audit interne, entreprise de télécommunications, Suède

« Un **risque émergent** pour les entreprises comme la nôtre concernent les réseaux sociaux et la relation avec les clients. Elle devient **de plus en plus importante**, car nous avons à notre disposition de nouveaux modes de **communication**, qui nous permettent de dialoguer plus facilement et **directement avec les clients** et d'autres cibles externes. Les réseaux sociaux ont permis, par rapport à l'époque où les médias de masse constituaient le principal canal de communication, de réduire la distance avec le public. Il est donc important que nous y **prêtions attention** ».

Responsable de l'audit interne, entreprise du secteur de l'habillement, Espagne

« La **pertinence** des messages, marqués par notre culture, que nous **communiquons** et diffusons dans le monde entier est une question importante. Nous avons vu des entreprises lancer des **campagnes marketing** qui ont choqué le public. Des identités culturelles ou religieuses peuvent être facilement heurtées, et les messages accueillis de manière défavorable peuvent facilement **nuire** à la **réputation** de l'organisation. »

Responsable de l'audit interne, entreprise de biens de consommation, Espagne



Début 2018, Mark Goldring, alors directeur général d'Oxfam, a réagi à un scandale concernant le comportement de collaborateurs à Haïti. Cette citation est un extrait du journal *The Guardian*. Cette interview a suscité de violentes réactions et il a été contraint de présenter ses excuses.

CULTURE ORGANISATIONNELLE : DISCRIMINATION ET INÉGALITÉS DE TRAITEMENT

L'ampleur des accusations de violences à l'encontre des actrices d'Hollywood qui a débuté en 2017 a été à l'origine du mouvement #MeToo. Le harcèlement, sur le lieu de travail ou dans l'ensemble de la société, n'est pas un phénomène nouveau. Néanmoins, le monde n'a jamais connu une telle pression pour faire changer ces attitudes par l'utilisation des réseaux sociaux permettant une large sensibilisation à cette question.

L'an dernier, la culture de l'organisation a fait son entrée parmi les thèmes à cibler, et elle demeure aujourd'hui un des principaux domaines de risques. A priori, tous les risques internes reposent sur le comportement des collaborateurs, à tous les niveaux, de la direction générale aux entités les plus opérationnelles. Notre sondage a montré que 25 % des répondants considéraient la culture comme un des cinq principaux risques de leur organisation, 6 % la plaçant en tête de leur classement. Le traitement équitable des collaborateurs et l'égalité sur le lieu de travail font partie de la culture organisationnelle, et nous avons découvert, au cours de notre enquête qualitative, que près de 10 % des personnes interrogées prévoyaient que la fonction d'audit interne s'intéresse de plus près à cette question à l'avenir.

Depuis quelques mois, des entreprises très médiatiques doivent apporter une réponse rapide au mouvement #MeToo. Étant donné l'importante proportion de plaintes émanant de l'industrie du spectacle aux États-Unis, il n'est pas surprenant qu'un service de diffusion de vidéos en ligne comme Netflix, qui produit ses propres contenus, se dote d'une politique de lutte contre le harcèlement et lance une campagne de sensibilisation contre les regards appuyés, les flirts et les étreintes sur le lieu de travail. Uber a dû abandonner une de ses conditions controversées qui exigeait que les plaintes pour harcèlement déposées à l'encontre de ses chauffeurs soient arbitrées de manière confidentielle ; les actions en justice peuvent dorénavant se dérouler en audiences publiques. Pendant ce temps, des cadres de Nike ont quitté l'entreprise après que des femmes travaillant pour le groupe de vêtements de sport ont fait circuler une enquête révélant de nombreux incidents et comportements inappropriés ainsi qu'une culture de l'organisation qui marginalise le personnel féminin et ne prend pas au sérieux les plaintes sur le lieu de travail.

Même si les exemples les plus frappants de la prise de conscience des phénomènes de harcèlement qui touche le monde des affaires depuis l'explosion du mouvement #MeToo viennent essentiellement des États-Unis, en Europe et ailleurs, les valeurs de l'organisation devront de plus en plus tenir compte de celles qui sont attendues au sein de la société. Les organisations doivent donc déterminer si elles sont exposées à une culture machiste toxique et à des comportements inappropriés qui portent atteinte à leurs collaborateurs et à la réputation de ces derniers. Cela doit se traduire par la mise en place de solides dispositifs d'alerte pour signaler certains abus. Les fonctions RH doivent également prendre les plaintes au sérieux, assurer un suivi des comportements inappropriés signalés et mettre en œuvre des politiques efficaces en matière de harcèlement, de diversité et d'inclusion.

Le code de gouvernance révisé du Royaume-Uni, qui doit entrer en vigueur en 2019, promeut la diversité au niveau des collaborateurs et la culture de l'organisation. Ce code actualisé comprend de nouveaux principes et dispositions sur la diversité et l'inclusion, ainsi que sur l'alignement des objectifs, de la stratégie, des valeurs et de la culture de l'organisation. Il spécifie également le rôle du conseil dans le pilotage et l'évaluation de la culture. De plus, un récent rapport du *Women and Equalities Committee* recommande que le gouvernement britannique prenne des mesures pour lutter contre le harcèlement sexuel sur le lieu de travail en proposant un certain nombre d'actions prioritaires, notamment l'introduction d'un devoir de prévention du harcèlement de la part de l'employeur. Les recommandations portent également sur le renforcement de l'application de la loi, un code de bonnes pratiques obligatoires et des dispositifs de contrôle plus efficaces concernant l'utilisation d'accords de non-divulgation utilisés pour réduire les victimes au silence.

Reporting sur les écarts de salaire

Du point de vue de l'entreprise, cette question relève de l'ESG (voir le chapitre Développement durable : éthique environnementale et sociale page 16), un thème plus vaste qui fait l'objet d'une incitation de plus en plus forte de la part des régulateurs et d'une attention externe. Les autorités exigent que les entreprises fassent preuve de plus de transparence dans leur façon de gérer les enjeux sociaux qui, à terme, les exposent également aux risques de réputation lorsque l'information est diffusée. Comme nous l'avons mentionné précédemment (voir page 16), la Directive européenne sur le reporting extra-financier requiert que les grandes entreprises publient des rapports

25 % des responsables de l'audit interne déclarent que la culture est un des cinq principaux risques auxquels leur organisation est confrontée...

...**10 %** sont convaincus que l'audit interne accordera une attention grandissante aux enjeux de discrimination et de traitement équitable des collaborateurs à l'avenir

Source : Sondage et entretiens réalisés auprès de nos membres

« Si vous cherchez les principaux enjeux pour 2019, vous ne pouvez pas passer à côté du **mouvement #MeToo**. Il s'agit d'une question morale, mais elle concerne aussi la manière dont les gens se comportent les uns envers les autres au sein de l'entreprise. Nous effectuons actuellement de nombreuses **enquêtes** dans des organisations où les mêmes problèmes que ceux soulevés par le mouvement #MeToo se posent, mais ils ne sont **pas rendus publics.** Il se pourrait que les auditeurs internes aient à s'y intéresser. Avant, ils se concentraient peut-être plus sur les missions financières, mais, aujourd'hui, ils doivent examiner tous les risques auxquels l'organisation est confrontée, et la **réputation** est un enjeu de taille ».

Responsable de l'audit interne,
cabinet de prestations externes, Pays-Bas

18 %
des hommes ont été victimes de comportements à caractère sexuel non désirés sur leur lieu de travail au Royaume-Uni

40 %
des femmes ont été victimes de comportements sexuels non désirés sur leur lieu de travail au Royaume-Uni

Source : enquête de la BBC

« Pour le moment, nous ne nous sommes pas intéressés à la manière dont les collaborateurs se comportent les uns avec les autres ou à la **discrimination liée au genre**. Il n'y a pas encore eu de demande en ce sens de la part du conseil et peu de cas nous ont été signalés. Mais je pense que ces sujets **entreront en ligne de compte** dans la mesure où ils correspondent à ce que la société juge **correct** et décent ».

Responsable de l'audit interne, groupe bancaire, Pays-Bas

28 %
des femmes ont déjà subi des commentaires à caractère sexuel au sujet de leur corps ou de leurs vêtements

35 %
des femmes ont déjà entendu des commentaires à caractère sexuel à propos d'autres femmes sur leur lieu de travail

Source : Trades Union Congress / Everyday Sexism Project

portant, entre autres, sur les politiques mises en œuvre en matière de traitement des collaborateurs et de diversité au sein des conseils.

Cette obligation de reporting s'intègre plus largement dans « l'engagement stratégique pour l'égalité hommes-femmes 2016-2019 » de la Commission européenne. Cette initiative a pour but de :

- accroître l'intégration des femmes au marché du travail et l'égalité de l'indépendance économique des femmes et des hommes ;
- réduire les écarts au niveau de la rémunération, des revenus et de la retraite, et ainsi lutter contre la pauvreté qui touche les femmes ;
- promouvoir l'égalité entre les femmes et les hommes dans le domaine de la prise de décision ;
- combattre les violences liées au genre, protéger et soutenir les victimes ;
- promouvoir l'égalité des genres et les droits des femmes à travers le monde.

Au niveau national, l'Allemagne et le Royaume-Uni ont déjà adopté des lois obligeant les entreprises cotées à communiquer dans leur rapport les écarts de salaire entre les hommes et les femmes. Au Royaume-Uni, les chiffres officiels montrent que dans 78 % des entreprises, les hommes sont mieux payés que les femmes, l'écart de rémunération médian se situant à 9,7 %. Pas moins de 1 500 entreprises britanniques n'ont pas respecté l'échéance de ce reporting fixée au 4 avril 2018. En plus des risques de conformité encourus, cette communication externe expose chaque entreprise à la vigilance accrue de l'opinion publique et à d'éventuelles critiques. Par exemple, bien que Body Shop emploie une majorité de femmes, il a été démontré que l'écart salarial dans cette chaîne de magasins est de 38,9 %.

En France, le président Emmanuel Macron a attribué en 2018 le label « grande cause nationale » à la Fédération Nationale Solidarité Femmes, un réseau de 65 organisations féministes, et il s'est engagé à réduire l'écart salarial qui s'élève à 25 %. La législation proposée obligerait les entreprises à combler tout écart de salaire dans un délai de trois ans, sous peine de se voir infliger une amende. En cas d'approbation par le Parlement, cette loi devrait entrer en vigueur d'ici 2020.

Une loi adoptée en 2018 stipule que les employeurs allemands ont l'obligation de communiquer en externe les détails concernant la rémunération de leurs collaborateurs et de justifier toute différence de salaire. Cette loi est comparable à celle adoptée par le législateur britannique. Toutefois, les entreprises allemandes sont encouragées à effectuer des missions d'audit interne sur les grilles de rémunération afin de s'assurer de leur conformité. Ces missions ne sont pas obligatoires, mais cette recommandation démontre clairement la valeur que la fonction d'audit interne peut apporter à la lutte contre les écarts de rémunération.

Du point de vue de l'audit interne

Les exigences réglementaires sont de plus en plus strictes en matière d'équité et d'égalité de traitement des collaborateurs. En Europe, cela s'est traduit par des exigences de communication externe dans les rapports des entreprises. Avant tout, la fonction d'audit interne peut aider les organisations à assurer qu'elles sont en conformité avec la réglementation, c'est-à-dire qu'a minima, la communication externe sur les écarts de salaire a été effectuée avant l'échéance réglementaire.

Au-delà des questions de conformité, la direction générale et le conseil devraient prendre très au sérieux toute forme de discrimination et d'inégalité sur le lieu de travail (misogynie, homophobie, transphobie, racisme, etc.). Cela devrait inclure la mise en place de politiques claires en matière de conduite, de rémunération et de sensibilisation élaborées en accord avec les ressources humaines et appliquées par cette fonction. Les DRH devraient également chercher à étayer les accusations et en effectuer le suivi.

La culture de l'organisation est devenue et continuera de constituer un enjeu majeur pour les entreprises, et les fonctions d'audit interne ont commencé à se pencher sur le sujet en s'intéressant à des aspects qualitatifs, comme la manière dont la direction générale s'assure que les valeurs de l'organisation se reflètent dans les comportements quotidiens ou qu'il n'y a pas d'incitations à des prises de risques excessives. Le harcèlement et les inégalités de traitement des collaborateurs sont sans aucun doute des problématiques culturelles. La fonction d'audit interne devrait donc intégrer ces éléments à son programme de travail en recherchant l'assurance que cet environnement toxique ne porte atteinte à aucun groupe démographique particulier sur le lieu de travail.

Questions clés

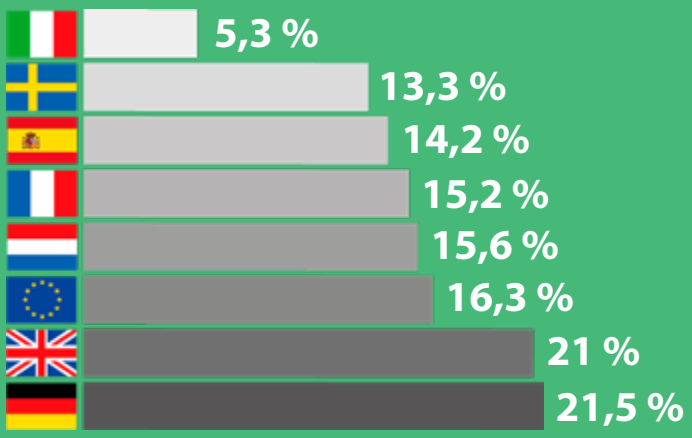
- La direction générale et le conseil sont-ils suffisamment attentifs aux évolutions sociales concernant le traitement équitable des femmes et des autres groupes démographiques marginalisés ?
- La direction a-t-elle « donné le bon ton » en matière de harcèlement ?
- L'organisation a-t-elle mis en place une politique claire et adéquate en matière de lutte contre le harcèlement ?
- L'organisation a-t-elle l'obligation de communiquer en externe les écarts de rémunération entre les hommes et les femmes ? Dans ce cas, est-elle en conformité avec la réglementation ? Et les données sont-elles exactes ?
- La DRH communique-t-elle cette politique, sensibilise-t-elle les collaborateurs, et assure-t-elle effectivement un suivi des accusations ?
- Des missions d'audit interne prennent-elles en compte les questions liées à la culture ? Dans ce cas, est-il possible d'y inclure des enquêtes et autres types d'évaluations qui pourraient éclairer la manière dont les collaborateurs sont traités au sein de l'organisation ?

« Nous devrions mieux prendre en compte la **diversité**, qui est un des thèmes d'actualité, ainsi que l'impact de cette diversité sur la performance des entreprises. Quoi que vous puissiez penser des **inégalités de rémunération entre hommes et femmes**, elles existent, et les organisations doivent y remédier. Dans des entreprises comme la nôtre, la composition des conseils doit absolument **être justifiée**. La diversité ne peut être que positive pour les organisations. Alors, comment la fonction d'audit interne peut-elle y contribuer ? Eh bien, quelle est la politique ? Comment est-elle déployée dans l'ensemble de l'organisation ? Quels sont les obstacles rencontrés ? Et les organisations sont-elles **réellement honnêtes** quand aux questions de diversité et à leurs objectifs dans ce domaine ?

Responsable de l'audit interne, établissement financier, Royaume-Uni

Écarts de rémunération entre hommes et femmes dans les principaux marchés européens

Source : Eurostat



-0,6 %

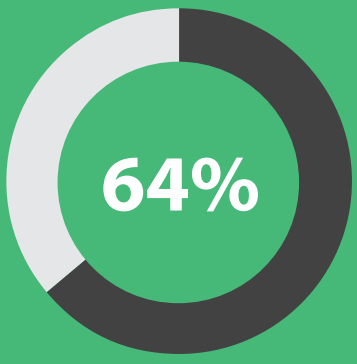
Au sein de l'UE, l'écart de rémunération n'a diminué que de 0,6 point de pourcentage depuis 2011

Source : Eurostat

28 %

L'écart de rémunération entre hommes et femmes s'élève à 28 % dans le secteur des services financiers dans l'Union Européenne. C'est le taux le plus élevé de tous les secteurs d'activité

Source : Eurostat



64 % des Européens sont favorables à la publication des salaires moyens par type de poste et par sexe dans leur entreprise

Source : Commission européenne

« L'audit interne devrait penser à la manière dont les première, deuxième et troisième lignes de maîtrise fonctionnent conjointement, et aux **moyens d'enquête** dont elle dispose ; qui devrait s'en charger, et quel est le niveau de coordination globale ? Ces questions peuvent être intégrées à des missions d'audit de la **culture** ; quelle est la culture de la hiérarchie et comment s'exerce-t-elle ? Et ces thèmes peuvent être élargis à une mission sur les questions liées au **genre** ou sur **l'égalité de rémunération**. Ce sont des sujets très intéressants, et les responsables de l'audit interne ont la possibilité de **donner l'élan** s'ils se chargent de ces questions ».

Responsable de l'audit interne, secteur public, Royaume-Uni

UNE NOUVELLE ÈRE COMMERCIALE : PROTECTIONNISME ET SANCTIONS

Le récent essor des politiques commerciales protectionnistes constitue un risque significatif pour les entreprises. Les États-Unis se sont engagés dans une bataille avec la Chine concernant la compétitivité des importations. Ces représailles réciproques se sont répercutées sur l'Europe et peuvent potentiellement faire baisser les ventes aux États-Unis, la plus grande économie du monde. À cela s'ajoute l'augmentation des sanctions commerciales qui entraînent de lourdes amendes.

Notre enquête qualitative a révélé qu'un répondant sur cinq considérait que l'impact potentiel du protectionnisme commercial et la nécessité de s'adapter à des mesures concernant les exportations constituaient d'importants domaines de risques. Nous n'avons pas pu dégager de tendance nationale, même si, comme on pouvait s'y attendre, la majorité (66 %) des répondants ayant mentionné ces problématiques exerçaient dans les secteurs de la construction, de l'industrie, de la distribution, des technologies de l'information et de la communication (c'est-à-dire des multinationales vendant des produits et services à l'échelle mondiale).

S'adapter à de nouvelles sanctions commerciales et éviter les amendes associées implique des risques réglementaires et/ou de conformité ; notre sondage a montré que ces deux thématiques étaient respectivement citées par 58 % et 37 % des responsables d'audit parmi les cinq principaux risques pour leurs organisations. Sur une base cumulée, ces domaines font partie des cinq risques les plus cités, aux côtés de la cybersécurité, de la sécurité des données et de la digitalisation.

Le protectionnisme commercial, à savoir la mise en place de taxes à l'importation, peut toutefois être considéré comme un risque politique pouvant nuire à la compétitivité et entraîner une perte de parts de marché ; 23 % des responsables d'audit ayant répondu à notre sondage ont cité l'incertitude politique comme un des cinq principaux risques.

L'an dernier, les risques politiques figuraient dans les thèmes à cibler en raison des incertitudes liées au Brexit, aux élections nationales en Europe et aux projets de Trump d'ériger des barrières commerciales. La sortie de la Grande-Bretagne de l'UE demeure un risque réel et d'actualité, mais il est fort probable que ce départ pèsera surtout sur les entreprises britanniques orientées vers l'exportation, et sans doute que les fonctions d'audit interne suivront de près l'évolution des négociations politiques et l'échéance qui arrive à grands pas. Au moment de l'élaboration de ce rapport, le Royaume-Uni et l'UE devaient encore s'accorder sur les conditions de ce départ.

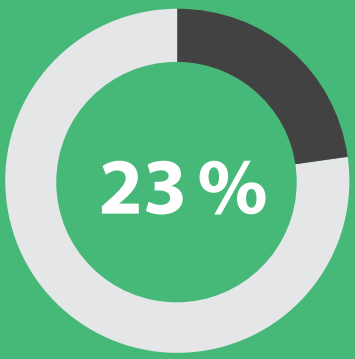
Les menaces commerciales proférées par l'administration Trump, véritables piliers de sa campagne électorale, sont aujourd'hui à l'œuvre. La Chine en a été, jusqu'ici, la cible principale. Le 15 juin 2018, les États-Unis ont publié une liste de produits chinois, d'une valeur de 50 milliards environ, qu'ils prévoient de taxer à 25%. La Chine a riposté en appliquant des mesures similaires. Les États-Unis ont alors dressé un deuxième inventaire de produits, d'une valeur de 200 milliards de dollars, pour lesquels les droits de douane s'élèveront à 10 %, ainsi qu'une liste supplémentaire prévue au cas où la Chine choisirait de répondre à nouveau. Cette guerre commerciale est désormais une réalité.

Mais la Chine n'est pas la seule à être victime de ces politiques : Les droits de douane sur les importations d'acier et d'aluminium, qui s'élèvent de 10 à 25 %, pèsent sur l'Europe, le plus gros exportateur de ces métaux vers l'Amérique, avec le Canada. Apportant une réponse considérée comme politique, l'UE a alors imposé un tarif douanier de 25 % sur des produits américains emblématiques tels que le bourbon et les motos Harley-Davidson. Si de nouveaux produits et matériaux subissent des droits et des taxes, en Europe, les entreprises pourraient voir leur chiffre d'affaires stagner ou chuter dans la mesure où ces marchandises ne seraient plus compétitives sur le marché nord-américain. Parallèlement, les coûts de production pourraient augmenter en raison de la majoration des prix des matières premières acquises aux États-Unis, ce qui exercerait une pression sur les marges.

A la suite de la mise en place de ces droits de douane, Donald Trump et Jean-Claude Juncker ont entamé des négociations préliminaires afin d'éviter qu'une véritable guerre commerciale n'éclate entre les États-Unis et l'Europe. Selon le président de la Commission européenne, l'objectif était de parvenir à un accord sur « zéro droit de douane, zéro barrière non tarifaire et zéro subvention sur les biens industriels hors automobile », suggérant ainsi que Trump proposerait de taxer les importations de voitures européennes. Le président américain a ajouté qu'il espérait résoudre la question des droits de douane sur l'acier et l'aluminium et des représailles au niveau de la politique douanière européenne.

Pour un responsable d'audit sur cinq, l'impact potentiel du protectionnisme commercial et la nécessité de respecter les mesures de contrôle des échanges avec certains pays sont probablement des risques à cibler en 2019 et dans les années à venir

Source : Entretiens réalisés auprès de nos membres



23 % des responsables d'audit considèrent l'incertitude politique comme un des cinq principaux risques auxquels leur organisation doit faire face

Source : Sondage réalisé auprès de nos membres

7 000 mesures de protectionnisme commercial correspondant à 400 milliards de dollars ont été introduites au cours des huit années qui ont suivi la crise financière. Ce chiffre n'inclut pas les récentes mesures imposées par Trump, qui comprennent 25 % de droits de douane sur des marchandises chinoises évaluées à 50 milliards de dollars.

Source : Gowling WLG

« La réglementation, y compris les **taxes à l'importation** envisagées par les États-Unis sur les produits européens, est un sujet de préoccupation. Je pense au secteur de l'automobile, mais c'est un problème général. Les droits de douane prévus par Trump toucheront plus fortement la grande consommation, et nous ne serons pas nécessairement affectés. Toutefois, les **États-Unis** représentent notre **marché le plus important** en termes de ventes. Cela pourrait donc néanmoins avoir une incidence sur nous, suivant la nature et la **précision** des **tarifs douaniers**. Il est trop tôt pour le dire, mais c'est une problématique que **nous devons surveiller** ».

Responsable de l'audit interne, constructeur automobile, Italie

« Les risques politiques sont une préoccupation majeure. La **potentielle guerre commerciale** que nous voyons se profiler nous affectera d'une manière ou d'une autre. Nous avons une longue **chaîne d'approvisionnement** à travers l'Europe et l'Asie. Les risques commerciaux liés aux réformes aux États-Unis et à la manière dont nous sécurisons nos **flux de marchandises** depuis la Chine jusqu'aux Pays-Bas en conservant des prix attractifs sont donc sans aucun doute des sujets de préoccupation, et ils pourraient devenir des **domaines de risques** nécessitant l'attention de la fonction d'audit interne ».

Responsable de l'audit interne, détaillant, Pays-Bas

L'Allemagne est le pays européen le plus susceptible d'être touché par les droits de douane en raison de la forte proportion d'entreprises exportatrices du pays, qui se traduit par un ratio commerce extérieur/PIB élevé (86 %).

Source : Banque mondiale

Jusqu'à présent, la présidence de Trump a été largement marquée par l'imprévisibilité des politiques élaborées par son administration. Si les négociations aboutissent, elles n'auront qu'un impact limité sur les exportateurs européens, mais les risques politiques en matière d'échanges commerciaux persisteront et les multinationales dotées de filiales aux États-Unis et en Chine pourraient avoir à supporter le coût financier de ces évolutions.

Impact des sanctions

À ces défis protectionnistes s'ajoutent les complications entourant les sanctions commerciales et économiques, qui émanent encore une fois des États-Unis. Elles se concentrent particulièrement sur l'Iran et la Russie ; les États-Unis se sont retirés de l'accord historique sur le nucléaire conclu en 2015, un retrait aux conséquences considérables sur le commerce avec l'Iran. Les États-Unis ont également introduit une série de sanctions à l'encontre des principaux oligarques russes, des sociétés leur appartenant, de représentants du gouvernement, et des entreprises publiques.

Ces évolutions peuvent avoir de graves conséquences inattendues, qui s'étendent bien au-delà des lourdes amendes encourues en cas de non-conformité. Par exemple, les sanctions prises en avril 2018 à l'encontre du producteur d'aluminium russe Rusal avaient pour objectif d'ébranler l'oligarque Oleg Deripaska, propriétaire de la société. Cette décision a perturbé le marché, faisant grimper les prix de l'aluminium, ce qui a nui aux constructeurs automobiles et aux autres fabricants. Les sanctions ont ensuite été assouplies, donnant ainsi aux entreprises le temps de rompre leurs liens avec Rusal.

Si les 18 premiers mois de la présidence Trump donnent un avant-goût de la suite des événements, les entreprises risquent d'être confrontées à des réformes réglementaires permanentes. L'an dernier, l'OFAC (*Office of Foreign Assets Control* ou Bureau du contrôle des avoirs étrangers) a placé 1 000 entités sur sa liste noire, soit près de 30 % de plus que lors de la dernière année de l'administration Obama, faisant des mesures de contrôle des exportations une cible mouvante devant constamment être surveillée. Cela a pour conséquence d'alourdir le fardeau lié aux questions de conformité pour les entreprises exposées aux marchés touchés.

Les effets des droits de douane ne se font pas toujours immédiatement sentir de manière évidente ou directe. Les organisations doivent avoir conscience des perturbations que ces tarifs douaniers peuvent causer, et décider en conséquence d'une éventuelle restructuration des chaînes d'approvisionnement. Les changements soudains qui affectent ces chaînes logistiques peuvent avoir un impact sur la qualité et la disponibilité des produits dans la mesure où les entreprises peuvent faire face à des difficultés lorsqu'elles s'efforcent de réduire la production dans certains sites et de l'augmenter dans d'autres. Il sera donc essentiel d'avoir une bonne visibilité sur les fournisseurs et les circuits d'approvisionnement afin de minimiser les perturbations et de maintenir les profits.

Du point de vue de l'audit interne

Que les risques liés au protectionnisme économique, aux sanctions commerciales et, plus généralement à la situation géopolitique, puissent être l'objet de missions d'audit est une question qui fait débat. Les gouvernements sont très réactifs, et il est difficile de prédire quels biens seront affectés et dans quelle mesure ils le seront, avant la publication des textes officiels. Toutefois, la fonction d'audit interne peut fournir une assurance sur la capacité de l'organisation à répondre aux changements de politiques et à mettre en œuvre des stratégies permettant de limiter les risques et de réagir en cas d'urgence.

Il est de plus en plus nécessaire d'évaluer les risques encourus tout au long de la chaîne d'approvisionnement, d'une région à l'autre, afin de définir les éventuels risques de perturbation de l'approvisionnement, d'augmentation des coûts et de baisse des ventes. La fonction d'audit peut y contribuer en soulignant l'importance de ces évaluations et en apportant à la direction générale et au conseil la preuve que l'organisation consacre suffisamment de temps et de ressources dans ce domaine, tout en garantissant qu'elle s'appuie sur les informations disponibles les plus récentes. Il n'est pas du ressort de la mission d'audit interne de décider de la pertinence d'une éventuelle restructuration de la chaîne d'approvisionnement, mais elle peut fournir un éclairage sur les processus d'évaluation des décisions stratégiques et de réaction aux risques politiques, et l'assurance que les impacts opérationnels sur les circuits d'approvisionnement sont pris en compte.

De la même manière, il est important de veiller à ce que les fonctions de conformité et d'achat de l'organisation veillent sur les mesures de contrôle des exportations et les sanctions y afférentes. Il s'agit avant tout de s'assurer que l'organisation évite les amendes, mais, au-delà de cela, les sanctions peuvent avoir un impact sur les prix du marché et la compétitivité. Le conseil peut donc exiger l'assurance que les travaux de conformité sont articulés aux processus d'élaboration des stratégies ; par exemple, l'interdiction des échanges commerciaux dans un marché prohibé incite-t-elle à pénétrer des marchés géographiques inexploités ?

Questions clés

- Dans quelle mesure et de quelle manière l'organisation peut-elle être affectée par les droits de douane (impact direct sur le chiffre d'affaires et/ou sur les coûts de production, perturbation de la chaîne d'approvisionnement, par exemple) ? La direction générale est-elle informée de cet impact potentiel ?
- L'organisation est-elle suffisamment flexible pour s'adapter à ces changements, en diminuant ses prix pour rester compétitive par exemple, ou le chiffre d'affaires est-il suffisamment réparti sur différents marchés, de sorte que l'impact des droits de douane américains reste minimal ?
- La chaîne d'approvisionnement doit-elle être restructurée ou l'organisation peut-elle supporter des coûts potentiellement plus élevés si elle n'effectue pas de modifications ?
- L'organisation réagit-elle aux changements de politiques commerciales en procédant régulièrement à des évaluations des risques ?
- Les fonctions de conformité et d'achat mettent-elles à jour le registre des sanctions commerciales et veillent-elles à ce qu'il soit respecté dans l'ensemble de l'organisation ?

Près de 1 000 entités et personnes ont été ajoutées à la liste noire des États-Unis durant la première année de l'administration Trump. Cela représente une augmentation de presque 30 % par rapport à la dernière année de la présidence Obama, et plus de trois fois plus que celles ajoutées pendant la première année de son mandat.

Source : Banque mondiale

« Les marchés dans lesquels nous sommes présents sont très **imprévisibles**, et il est difficile de prédire la manière dont ils pourraient être touchés par les sanctions américaines. Nous sommes présents en **Russie** et les **mesures de contrôle des exportations** sont sans cesse en évolution, dans un sens ou dans un autre. Si nous voulons nous **développer** dans de nouveaux pays, nous devons être très attentifs à l'évolution probable de la situation d'ici à **cinq ans** ; pouvons-nous être certains que le **système politique** est stable, qu'il n'existe pas de conflits politiques, et que le pays n'est pas susceptible d'être **sanctionné** ? »

Responsable de l'audit interne, groupe de distribution, Allemagne

« Les mesures de contrôle des exportations et les sanctions qui en découlent ont toujours existé, mais maintenant que le régime de sanctions est plus **étendu**, en particulier de la part des États-Unis vers des pays comme l'**Iran** et la **Russie**, ils sont devenus une préoccupation majeure. Le Bureau du contrôle des avoirs étrangers du département du Trésor des États-Unis, qui **poursuit** ce type de violations, applique des **amendes sévères**. Des sanctions sont imposées à l'Iran et, si vous vous renseignez auprès des acteurs principaux, vous verrez qu'ils cherchent tous à vendre leurs produits au **Moyen Orient** ».

Responsable de l'audit interne, éditeur de logiciels, Allemagne

+10 $

La décision de Trump d'imposer de nouvelles sanctions sur l'Iran semble avoir joué un rôle majeur dans la hausse du baril d'environ dix dollars qui a touché le secteur pétrolier depuis la mi-mars. Cette augmentation entraînera une pression inflationniste sur les coûts de production des entreprises

Source : HSBC

2 087 207 524 $

Durant les cinq dernières années, le Bureau du contrôle des avoirs étrangers du département du Trésor des États-Unis a imposé 90 amendes, d'une valeur de plus de 2 milliards de dollars, pour violation avérée des sanctions économiques et commerciales.

Source : Holland & Hart

GOUVERNANCE DES RISQUES ET DES CONTRÔLES : S'ADAPTER AU CHANGEMENT

Le rythme d'évolution des activités et des risques auxquels les entreprises sont exposées n'a jamais été aussi rapide. Alors qu'elles s'adaptent pour assurer leur croissance, les normes de gouvernance des risques et les environnements de contrôle, conçus pour couvrir les risques d'hier, peuvent rapidement devenir obsolètes.

Lors de nos entretiens, une personne sur dix a souligné la nécessité d'évaluer ou de réévaluer les approches de leur organisation en matière de gouvernance des risques et de structuration des dispositifs de contrôle. Cela peut sembler évident. L'objectif de l'audit interne est de fournir une assurance au conseil et aux membres du comité d'audit en ce qui concerne la gouvernance, les risques et le contrôle interne, dans tous les domaines de l'organisation. Pour ce faire, les auditeurs internes testent et évaluent les principaux dispositifs de contrôle et processus au niveau d'une unité opérationnelle ou à l'échelle de l'organisation. Ces travaux devraient donner une vision globale de la capacité de l'organisation à adapter et à mettre à jour son environnement de contrôle.

Il n'a jamais été aussi urgent de modifier les dispositifs de contrôle et de déployer une gestion efficace des risques pour maîtriser les aléas actuels et futurs et optimiser la création de valeur. Les contraintes réglementaires nationales et internationales sont de plus en plus complexes, les évolutions de rupture dans leurs marchés obligent les entreprises établies à adapter rapidement leurs modèles économiques et leurs stratégies, les fusions et les acquisitions passent par la juxtaposition de différents environnements de contrôle, les activités opérationnelles sont de plus en plus externalisées, et les processus sont rationalisés et accélérés avec la digitalisation. Ceci requiert d'introduire de nouveaux dispositifs de contrôle et d'affiner ceux qui sont déjà en place afin de s'assurer que les risques associés continuent d'être gérés de manière adéquate. C'est en ce sens que la maîtrise des risques est un domaine en constante évolution.

Certaines modifications de dispositifs de contrôle et processus internes, telles que celles requises par les lois et règlements, sont obligatoires. La récente introduction du RGPD est un bon exemple d'une évolution réglementaire imposant un changement à grande échelle des dispositifs de contrôle interne des organisations. Toutefois, dans de nombreux cas, la conception et la mise en œuvre de systèmes de contrôle rigoureux peut prendre du retard par rapport au rythme auquel les entreprises évoluent.

Par exemple, les organisations continuent de migrer vers le *cloud* des logiciels et des données sensibles, qui étaient auparavant stockés sur des serveurs internes. Un plan de continuité d'activité (PCA) antérieur peut avoir prévu le passage à un serveur de secours sur site en cas de panne de réseau, mais il est probable que cela ne soit plus possible et, si la politique de continuité d'activité n'a pas été mise à jour, les opérations de l'entreprise pourraient être arrêtées si les prestations de service *cloud* sont interrompues. Dans ce cas de figure la mise à jour du PCA est donc nécessaire.

Bien évidemment, il n'est pas de la responsabilité de la fonction d'audit interne de concevoir ou de déployer l'environnement de contrôle ; cela constituerait un conflit d'intérêts majeur et porterait atteinte à l'indépendance et à l'objectivité de la troisième ligne de maîtrise. Pour autant, la fonction d'audit interne peut aller au-delà de l'évaluation de contrôles spécifiques censés atténuer des risques particuliers et donner une vision globale de l'efficacité et de la réactivité de la première ligne dans la conception et la mise en œuvre de nouveaux dispositifs de contrôle au sein de l'organisation. Autrement dit, le processus de conception des dispositifs de contrôle est-il suffisamment souple et réactif, ou l'environnement de contrôle est-il dans l'ensemble faible et rapidement dépassé ?

Innovation agile

C'est un enjeu particulièrement pertinent pour les entreprises les plus innovantes, qui investissent de manière importante dans le développement de nouvelles applications et autres technologies qui pourront ensuite être plus largement déployées au moment opportun, que ce soit pour être vendues ou être utilisées en interne.

Les entreprises utilisent des méthodes de développement en mode agile pour accélérer le rythme de l'innovation et la mise en marché. Cette approche « allégée » *(lean)* permet à des équipes pluridisciplinaires autonomes, et dans certains cas à des utilisateurs finaux, de développer des technologies et autres produits. Elle se caractérise par des cycles de développement incrémentaux et rapides ; selon les estimations, les entreprises qui utilisent des approches agiles à grande échelle ont accéléré leur rythme d'innovation de plus de 80 % [7].

Selon les principes de la méthode agile, l'accent est mis sur :

- les individus et les interactions plutôt que les processus et les outils ;
- un logiciel qui fonctionne plutôt qu'une documentation exhaustive ;
- la collaboration avec les clients plutôt que la négociation contractuelle ;
- l'adaptation au changement plutôt que l'application d'un plan prédéfini.

Ces méthodes peuvent sembler en contradiction avec l'approche orientée processus et contrôles de l'audit interne. Il peut donc être difficile d'apprécier la valeur ajoutée de l'audit interne dans un environnement fondé sur un niveau d'autonomie très élevé, un dispositif de gestion des risques a minima ou des contrôle souples. Cependant, l'audit peut jouer son rôle de conseil à propos des « risques de conception ». Plutôt que d'adapter a posteriori des dispositifs de contrôle à une nouvelle application ou technologie, la fonction d'audit interne peut prendre part, dès le départ, au processus de développement, et apporter des points de vue et son savoir-faire spécifiques, aidant ainsi l'organisation à éviter les pièges éventuels. Ainsi, l'intégration du service ou du produit dans l'environnement de contrôle est facilitée.

Il sera également de plus en plus important d'être en mesure de fournir une assurance quant à la capacité d'innovation de l'organisation. En effet, la direction générale peut souhaiter avoir une idée de la performance globale des processus d'innovation et de leurs lacunes. La question de l'alignement des stratégies d'innovation avec la stratégie globale de l'entreprise est au cœur des missions d'audit dans ce domaine. Cet alignement est-il pris en considération dans l'ensemble de l'organisation, les projets sont-ils suivis, examinés et évalués de manière efficace, les différents collaborateurs et services communiquent-ils et collaborent-ils efficacement, et comment les résultats des développements (c'est-à-dire les produits ou applications) sont-ils intégrés dans l'entreprise ?

Savoir mesurer l'efficacité des approches agiles et d'autres méthodes de développement en termes de création de valeur et, avec du recul, l'impact de l'évolution constante des structures organisationnelles sur la gouvernance des risques et l'environnement de contrôle global sont des défis majeurs pour les organisations et les fonctions d'audit interne.

Questions clés

- Quelle est la qualité globale de la gouvernance et du management des risques, par exemple, la deuxième ligne de maîtrise est-elle globalement efficace, quelles sont ses activités courantes, et réagit-elle face au changement ?
- L'organisation a-t-elle subi ou prévoit-elle de subir des modifications importantes au cours des trois dernières/prochaines années ? Quelles sont ces modifications (co-entreprise, digitalisation, développement d'applications, etc.) ? Le référentiel de contrôle interne nécessite-t-il d'être adapté en conséquence ?
- La conception et la mise en œuvre des dispositifs de contrôle répondent-elles à ces changements et à la croissance de l'organisation ?
- Quel impact l'introduction des technologies a-t-elle sur l'environnement de contrôle ?
- Les dispositifs de contrôle inefficaces et redondants, à faible valeur ajoutée en termes de maîtrise des risques, sont-ils abandonnés ou remplacés ?
- La fonction d'audit interne est-elle capable de maîtriser les changements organisationnels et leur incidence sur l'environnement de contrôle ?
- L'organisation utilise-t-elle des méthodes de développement agiles et aboutissent-elles aux résultats prévus tout en permettant de maîtriser les risques futurs ? Cette approche agile est-elle efficacement coordonnée ou est-elle cloisonnée et dispersée ?
- La fonction d'audit interne peut-elle apporter une valeur ajoutée en donnant des conseils sur l'examen des risques dès les phases amont du développement ?

« Nous vision une **simplification** réelle de l'environnement de contrôle. Le système de contrôle actuel est **trop compliqué** et il met trop l'accent sur la légalité et la conformité. Avec notre nouveau système informatique intégré et nos nouvelles procédures organisationnelles, c'est le moment idéal pour toutes les parties prenantes de mettre intelligemment tout à plat pour essayer de trouver des **dispositifs de contrôle plus fluides** au service des activités opérationnelles ».

Responsable de l'audit interne, secteur public, France

« La fonction d'audit interne se focalise souvent sur les anciennes structures organisationnelles et leur **gouvernance des risques**. Mais nous évoluons plutôt vers des organisations en réseaux et **des développements agiles**. Avons-nous les ressources nécessaires pour mener des évaluations dans ce nouveau contexte ? Pouvons-nous aborder les dispositifs de contrôle, les documents de pilotage et l'ensemble de **l'évaluation** comme nous le faisions par le passé ? La fonction d'audit interne doit-elle **adapter son approche** lorsque que des développements sont menés en mode agile ? »

Responsable de l'audit interne, groupe de télécommunications, Suède

AUDITER LES RISQUES-CLÉS : ADOPTER UNE VÉRITABLE APPROCHE FONDÉE SUR LES RISQUES

Il existe un certain décalage entre les domaines de risques prioritaires des organisations et ceux auxquels la fonction d'audit interne consacre son temps. Les responsables d'audit devraient donc réévaluer avec les membres du comité d'audit et les parties prenantes si l'audit interne est utilisé de manière efficace pour fournir une assurance solide fondée sur une approche par les risques.

L'un des constats les plus étonnants de notre sondage est l'écart entre les risques les plus importants pour l'organisation et ceux auxquels les fonctions d'audit interne consacrent leur temps. Par exemple, 15 % des répondants considèrent que la cybersécurité constitue le risque majeur pour leur organisation et 66 % l'ont placée parmi les cinq risques prioritaires, mais seulement 5 % ont déclaré y consacrer la plus grande partie de leur temps. Par ailleurs, 13 % ont classé la conformité comme le principal risque de leur organisation et 58 % dans le top 5, mais 33 % affirment y passer le plus clair de leur temps.

En d'autres termes, alors que le caractère prioritaire de la cybersécurité est partagé, le temps passé sur les questions de conformité est largement plus élevé. Cette observation soulève la question de savoir si la mission d'audit interne adopte une véritable approche fondée sur les risques.

Il est important de noter que cet écart peut s'expliquer de diverses manières, et ces dernières devraient être prises en compte avant de tirer toute conclusion définitive. Il est par exemple possible que :

- les responsables de l'audit interne et les membres du comité d'audit n'allouent pas efficacement le temps et les ressources de la mission d'audit aux risques les plus importants pour l'organisation. Autrement dit, la fonction d'audit n'adopte pas une approche suffisamment fondée sur les risques ;
- l'audit interne ait à effectuer des travaux obligatoires, comme des audits de conformité qui peuvent être surtout prioritaires pour les régulateurs mais moins pour l'organisation ou la fonction d'audit ;
- le conseil / les membres du comité d'audit et les responsables de l'audit interne aient une perception différente des risques prioritaires pour l'organisation (cette question devrait être abordée au moins une fois par an avec la direction générale et le conseil lorsque le plan d'audit fondé sur une approche par les risques est revu et approuvé) ;
- le temps alloué à certaines missions d'audit est dépassé au détriment d'autres domaines de l'organisation ;
- l'assurance relative à certains risques prioritaires ne soit pas, ou pas uniquement, fournie par la fonction d'audit interne (elle peut être confiée à la deuxième ligne ou externalisée par exemple) ;
- certains domaines de risques élevés ne puissent pas en pratique faire l'objet d'une mission d'assurance et ne nécessitent qu'un avis ou des conseils qui peuvent être moins chronophages (par exemple sur les risques liés à l'incertitude politique).

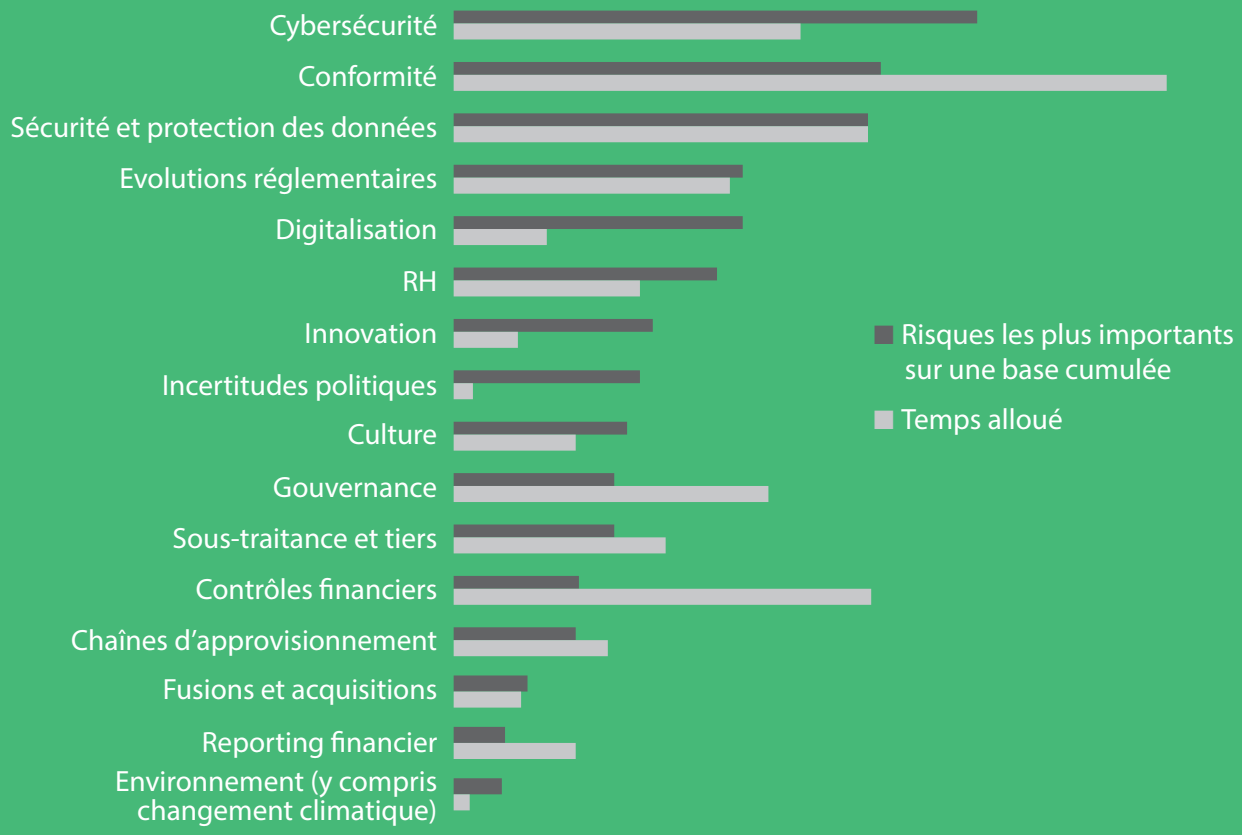
Quelles que soient les raisons de ce constat, il est crucial que les responsables de l'audit interne soient certains que leur fonction donne la meilleure assurance possible en prenant en compte les principaux risques potentiels de leurs organisations.

Les entreprises subissent une pression constante qui les pousse à innover, à s'implanter sur des marchés connexes et sur de nouveaux territoires, à adapter leurs modèles économiques et à se transformer continuellement pour rester compétitives. Le défi de la concordance entre les travaux d'assurance de la troisième ligne de maîtrise et les risques majeurs pour l'organisation est donc plus difficile à relever à mesure que les univers de risques s'élargissent et que les attentes en matière d'audit interne augmentent. Il existe un risque que l'audit interne ne soit pas utilisé pour faire face efficacement aux enjeux d'aujourd'hui et de demain, mais plutôt pour répondre à ceux d'hier. Si tel est le cas, le responsable de l'audit interne devrait combler cette lacune en matière d'assurance en discutant avec le comité d'audit. En effet, selon l'un des principes fondamentaux du Cadre de référence international des pratiques professionnelles de l'audit interne, cette fonction doit être en phase avec la stratégie, les objectifs et les risques de l'organisation. Ce principe est applicable, qu'il s'agisse de l'adoption de l'intelligence artificielle, du développement de nouveaux marchés ou d'un autre but stratégique.

Les bénéfices de l'innovation

Un audit interne véritablement fondé sur une approche par les risques ne consiste pas uniquement à identifier correctement les principaux risques encourus par l'organisation, mais également à gérer efficacement le temps et les ressources. Il s'agit d'un défi permanent pour la fonction d'audit interne qui peut être surmonté en améliorant les compétences et en adoptant des techniques d'analyse de données dans le cadre d'un audit en continu. L'analyse de données n'a pas seulement la capacité de libérer du temps pour la mission d'audit interne, elle permet également d'effectuer des tests sur l'ensemble de la population et donc d'offrir des niveaux d'assurance plus élevés dans des domaines

Notre sondage révèle qu'il existe une inadéquation entre les risques les plus importants aux yeux des responsables d'audit et ceux auxquels les fonctions d'audit interne consacrent leur temps



« C'est un vrai défi de réussir à **équilibrer** les risques avec le temps que nous y allouons. L'entreprise achète et vend des actifs, **le plus important** est donc que nous le fassions bien, que le cycle se perpétue et que la valeur nette des actifs augmente avec le temps. Nous **ne passons pas** beaucoup de **temps** à examiner les propositions d'investissement et à déterminer si nous vendons aux bons acheteurs et au bon prix. Ce processus est **bien rodé**, et on peut donc s'interroger sur la valeur que nous pourrions en retirer, même si nous pouvons certainement en tirer quelque chose. Nous avons plutôt tendance à examiner d'autres éléments **indirectement liés** à la valorisation, comme la qualité de gestion du portefeuille ».

Responsable de l'audit interne, gestionnaire de placements alternatifs, Royaume-Uni

« L'organisation essaie de trouver le bon équilibre avec la réglementation. Nous sommes une entreprise cotée et nous devons nous conformer aux réglementations du marché des actions et à celles du marché obligataire. Les organismes de contrôle exercent des pressions et nous le comprenons, mais nous voulons faire les choses correctement pour valoriser ce processus. Cela nécessite que nous menions des missions d'audit plus formelles et documentées qui ne sont pas nécessairement fondées sur les risques ; elles ne correspondent alors pas à ce que la direction générale et les membres du comité d'audit attendent de nous. Ce qu'ils veulent, c'est comprendre comment va l'entreprise. Nous n'accordons pas une grande valeur aux audits de conformité, si ce n'est pour s'assurer que l'organisation est conforme, alors que que la valeur réelle réside dans d'autres processus et plans d'activité *(business plan)* de la mission d'audit. C'est un équilibre difficile à atteindre ».

Responsable de l'audit interne, entreprise multinationale de construction, Espagne

tels que la vérification des comptes créditeurs et des états de paie.

On estime qu'environ 76 % des fonctions d'audit interne utilisent actuellement l'analyse de données dans le cadre du processus d'audit. Toutefois, parmi le quart restant, plus d'un tiers (34 %) ne prévoient pas d'intégrer de tels outils [8], une situation qui sera de plus en plus intenable à mesure que les organisations continueront de numériser leurs opérations, qu'il s'agisse des services au contact des clients ou du back-office.

Bien évidemment, l'analyse de données n'est pas une panacée, et des données de bonne qualité sont essentielles pour qu'un audit en continu soit efficace. Cependant, avec les compétences et les données adéquates, il est possible d'évaluer plus efficacement les risques et les dispositifs de contrôle, et d'avoir une couverture plus large et plus approfondie, en y consacrant moins de temps ; c'est-à-dire « faire plus avec moins ». Appliqué à des domaines tels que la conformité et les contrôles financiers, l'audit en continu fondé sur l'analyse de données peut permettre de dégager du temps pour que les auditeurs internes se concentrent sur des domaines de risques élevés auxquels ils accordent moins d'attention, comme la cybersécurité et les risques stratégiques.

L'articulation des lignes

Une autre solution réside dans un partenariat plus étroit et un partage plus efficace de l'information entre la deuxième et la troisième ligne. En effet, utiliser l'évaluation des risques de la deuxième ligne de maîtrise pour alimenter le plan d'audit interne peut contribuer à assurer que cette troisième ligne se concentre sur les secteurs les plus prioritaires. Il peut même être possible de décharger la troisième ligne de certains travaux d'assurance (pour les confier à la deuxième ligne ou à des tiers dans le cadre d'une co-traitance) pour que la fonction d'audit interne puisse se concentrer sur des domaines où son intervention est plus nécessaire. Dans tous les cas, les responsables de l'audit interne devraient coordonner et documenter les activités avec d'autres prestataires d'assurance internes et externes, au moyen d'une cartographie des prestations d'assurance, afin d'assurer une couverture adéquate et d'éviter les doubles emplois, comme le souligne la norme 2050 du Cadre de référence international des pratiques professionnelles de l'audit interne.

Il convient néanmoins d'être attentif à la répartition des rôles entre les lignes. Notre sondage montre que 29 % des fonctions d'audit interne réalisent des activités de management des risques. Ce chiffre n'est pas préoccupant en soi, mais 38 % de ces répondants assument des rôles de la deuxième ligne dans lesquels ils ne devraient pas être impliqués.

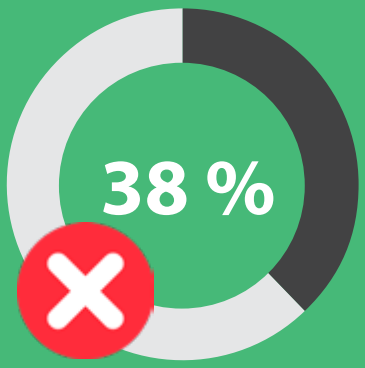
Ces responsabilités incluent, entre autres, le devoir de rendre compte concernant le management des risques, la définition de l'appétence pour le risque et la prescription de processus de management des risques. Assumer de tels rôles porte sérieusement atteinte à l'objectivité de la fonction d'audit interne et devrait à tout prix être évité. L'appétence pour le risque doit toujours être établie par le conseil et, conformément à la norme internationale 1112, lorsque le responsable de l'audit interne assume des rôles qui ne relèvent pas de la mission d'audit, des précautions doivent être prises pour limiter les atteintes à l'indépendance et à l'objectivité. En tant que responsable d'audit, si vous considérez que certaines responsabilités que vous assumez en matière de management des risques compromettent votre objectivité, vous devriez en discuter immédiatement avec le conseil, et toute activité source de conflit d'intérêts devrait être allouée de manière appropriée entre la deuxième et la troisième ligne de maîtrise.

Questions clés

- En tant que responsable de l'audit interne, pensez-vous que le temps que la fonction d'audit consacre aux différentes activités correspond aux risques les plus importants pour l'organisation ?
- Si vous observez un écart, comment s'explique-t-il ? Par exemple, une autre fonction fournit-elle l'assurance nécessaire ?
- Le conseil / les membres du comité d'audit et les responsables de l'audit interne ont-ils une perception différente des risques prioritaires pour l'organisation ? Si tel est la cas, comment cet écart s'explique-t-il et cette question est-elle régulièrement discutée ?
- En tant que responsable de l'audit interne, avez-vous un plan stratégique d'audit interne fondé sur les risques revu, partagé et discuté au moins une fois par an avec le comité d'audit ?
- Est-il possible d'accroître les capacités en matière d'analyse de données pour réaliser des missions d'audit en continu dans des domaines de risques plus matures, comme les contrôles financiers ?
- Les activités d'audit interne sont-elles coordonnées avec des prestataires d'assurance internes et externes pour assurer une couverture adéquate ?
- Existe-t-il une cartographie des prestations d'assurance formalisant clairement la répartition des responsabilités et le devoir de rendre compte en matière d'assurance pour l'ensemble des principaux risques de l'organisation ?
- La fonction d'audit interne assume-t-elle des rôles et des responsabilités de la deuxième ligne qui portent atteinte à son objectivité et détournent son attention des principaux risques ayant un niveau de couverture insuffisant ?

29 % des fonctions d'audit interne réalisent des activités de management des risques

Source : Sondage réalisé auprès de nos membres



38 % des fonctions d'audit interne assument des rôles dans lesquels ils ne devraient pas être impliqués

Source : Sondage réalisé auprès de nos membres

Principaux rôles de l'audit interne en matière de gestion des risques de l'entreprise	Rôles légitimes de l'audit interne avec des précautions	Rôles que la fonction d'audit interne ne devrait pas assumer

Source : Prise de position de l'IIA « Le rôle de l'audit interne dans le management des risques de l'entreprise »

SOURCES

1. Cybersecurity Ventures — 2017 Cybercrime Report: bit.ly/CyberVentures2017
2. Symantec — Internet Security Threat Report: www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
3. Bild am Sonntag report: www.bild.de/wa/ll/bild-de/unangemeldet-42925516.bild.html
4. Reuters/Ipsos — Americans less likely to trust Facebook than rivals on personal data: bit.ly/FacebookTrust
5. Cisco — The Zettabyte Era: www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html
6. OECD — 2016 Data on Enforcement of the Anti-Bribery Convention: www.oecd.org/daf/anti-bribery/Anti-Bribery-Convention-Enforcement-Data-2016.pdf
7. McKinsey — An operating model for company-wide agile development: www.mckinsey.com/business-functions/digital-mckinsey/our-insights/an-operating-model-for-company-wide-agile-development
8. Protiviti — Analytics in auditing is a game changer: www.protiviti.com/sites/default/files/2018-internal-audit-capabilities-and-needs-survey-protiviti.pdf