RISQUES A CIBLER

LES SUJETS INCONTOURNABLES DE L'AUDIT INTERNE EN 2018

RAPPORT ETABLI PAR DES INSTITUTS EUROPÉENS D'AUDIT INTERNE

TABLE DES MATIÈRES

Associazione Italiana Internal Auditors

Chartered Institute of Internal Auditors

Switzerland

ifaci institut français de l'audit et du contrôle internes

Instituto de Auditores Internos de España

Instituut van Internal Auditor Nederland

LES SUJETS INCONTOURNABLES DE L'AUDIT INTERNE EN 2018

En 2016, l'IFACI, l'IIA Italie et l'IIA Espagne ont publié « Les sujets incontournables pour l'audit interne 2017 ». Cette année, un groupe plus important d'Instituts européens d'audit interne ont adopté une approche ambitieuse, en interrogeant des responsables de l'audit interne d'organisations majeures dans six pays européens – l'Espagne, la France, l'Italie, les Pays-Bas, le Royaume-Uni et la Suisse – pour avoir en ligne de mire les thèmes clés sur lesquels l'audit interne doit porter son attention pour contribuer à la maîtrise des risques, protéger leurs organisations et apporter de la valeur ajoutée.

Ces sujets incontournables ont été identifiés grâce à des entretiens qualitatifs approfondis avec des responsables de l'audit interne représentant un large éventail de secteurs clés – construction/infrastructure, établissements financiers, système d'information, industrie, secteur public, distribution, télécoms, services publics et énergie – et d'organisations leaders dans ces secteurs. Pour une mise en perspective, ces organisations ont une capitalisation boursière cumulée supérieure à 724 milliards d'euros, un chiffre d'affaires de plus de 441 milliards d'euros, emploient plus de 1,86 million de personnes et sont présentes dans pas moins de 173 pays. Rien que dans le secteur des établissements financiers, les responsables de l'audit interne représentent des entreprises qui valent collectivement plus de 325 milliards d'euros et qui ont un bénéfice annuel de plus de 207 milliards d'euros.

Nous sommes sincèrement reconnaissants à ceux qui ont participé à notre recherche. Leurs connaissances et leurs points de vue offrent un instantané précieux de la réflexion d'éminents professionnels de l'audit interne à travers l'Europe.

Les sujets incontournables proposés dans ce rapport reflètent les domaines de risques auxquels les responsables de l'audit interne donnent la priorité alors qu'ils préparent leurs plans d'audit pour 2018 et procèdent aux évaluations des risques à plus long terme. Pour certains lecteurs, leurs plans d'audit pour l'année renvoient déjà à ces thèmes. Ils voudront peut-être utiliser notre recherche pour souligner auprès de leurs comités d'audit qu'ils sont effectivement sur la bonne voie. Pour d'autres, ce rapport peut servir à rappeler ces problématiques qui méritent une sérieuse attention lors de la finalisation de leur plan 2018 ou à plus long terme. Nous espérons que notre publication offrira à chacun un sujet de discussion nouveau et pertinent, à la fois pour les professionnels de l'audit interne et pour les comités d'audit et les autres parties prenantes.

Diversité et évolution

Les risques ne sont pas statiques et même les plans d'audit les plus cadrés évoluent avec les nouveaux risques qui émergent au niveau opérationnel, stratégique et dans l'environnement. En outre, ce qui constitue une menace potentielle pour une organisation peut être jugé inconséquent par une autre. Ceci étant, le domaine de risques le plus communément identifié par les responsables de l'audit interne tous secteurs et nationalités confondus est la cybersécurité. Ce n'est pas une surprise, étant données l'ampleur de la menace et la mesure dans laquelle toutes les organisations dépendent des technologies. Ce thème est suivi par le Règlement général sur la protection des données et l'enjeu plus vaste de la gestion des données ; le rythme des innovations auxquelles les organisations doivent faire face vient en troisième position.

Les priorités des responsables de l'audit interne diffèrent selon les secteurs et, dans une moindre mesure, les pays. Ainsi, l'incertitude politique est beaucoup plus fréquemment citée par les responsables de l'audit interne d'organisations basées au Royaume-Uni, sans doute dans la perspective du Brexit et des impacts potentiels des négociations qui commencent. Les responsables de l'audit interne espagnols citent également l'incertitude politique comme un domaine qui pourrait exposer leurs organisations à des risques émergents, mais aussi à des opportunités. En particulier, pour les multinationales installées au Mexique et potentiellement concernées par les positions hostiles de l'administration de Trump envers ce pays.

Les responsables de l'audit interne d'établissements financiers sont les plus préoccupés par la complexité de la réglementation. Il est vrai que des règlements spécifiques ont été récemment mis en application, ou sont imminents, dans toute l'Union européenne. Les responsables de l'audit interne d'établissements bancaires en France, en Italie, aux Pays-Bas et en Espagne, doivent en particulier intégrer les attentes de la Banque centrale européenne dans le cadre du mécanisme de surveillance unique entré en vigueur il y a trois ans et qui continue de se développer.

Cependant, le message clé de ce rapport est l'impact fondamental des technologies qui déterminent, facilitent et bouleversent les opérations et les stratégies des organisations. Une pression qui incite les auditeurs internes à acquérir de nouvelles compétences et à adopter des outils innovants afin de renforcer leurs capacités dans un monde de plus en plus numérique.

Nous espérons que vous apprécierez ce rapport, vos réactions sont les bienvenues et nous vous remercions de votre intérêt.

RGPD : L'ENJEU DE LA PROTECTION DES DONNÉES

Le Règlement général sur la protection des données (RGPD) aurait pu être traité avec les questions de conformité ou de cybersécurité. Cependant, cette nouvelle exigence mérite une attention spécifique pour un certain nombre de raisons.

La portée du RGPD est inégalée parce que les données personnelles sont tellement omniprésentes que pratiquement toutes les organisations d'une certaine taille traitent ou détiennent des quantités substantielles d'informations concernant leurs clients et leurs collaborateurs. De plus, la date limite pour la mise en conformité approche rapidement (la mise en œuvre est requise d'ici le 25 mai 2018). Enfin, et c'est peut-être le plus important, les pénalités pour non-conformité sont potentiellement énormes : pour les violations les plus préjudiciables, des amendes jusqu'à 4 % du chiffre d'affaires annuel ou 20 millions d'euros, en fonction du montant qui sera le plus élevé, pourraient être imposées.

A titre d'exemple, l'amende de 400 000 £ imposée par le bureau du Commissaire à l'information britannique au groupe TalkTalk dans le secteur du haut débit, pour ses manquements médiatisés à la sécurité des données il y a deux ans, aurait pu atteindre la somme astronomique de 59 millions de livres sterling[1] en application du RGPD.

En outre, un sondage récent auprès de 900 décideurs du monde entier indique que seuls 31% d'entre eux considèrent que leur organisation est en conformité avec le RGPD, alors qu'une étude montre que seules 2% des organisations semblent être totalement en conformité[2].

Les conseils devraient avoir déjà fait du RGPD une priorité compte tenu de l'ampleur des enjeux financiers des non-conformités et des travaux à accomplir pour parvenir à une conformité totale. Quels que soient les progrès déjà accomplis, l'audit interne a un rôle important à jouer pour évaluer la conformité à compter du 25 mai 2018.

Au-delà de la sécurité

Ce règlement prévoit un renforcement du rôle des mesures de sécurité comme des pare-feu et un chiffrement performants, et oblige les sociétés (les contrôleurs des données) à signaler toute violation de données à caractère personnel dans les 72 heures, même si elle a lieu au niveau d'un tiers (service de traitement des données). Pour cela, il sera nécessaire que la protection des données et les mesures de gouvernance soient inscrites dans les contrats avec les fournisseurs.

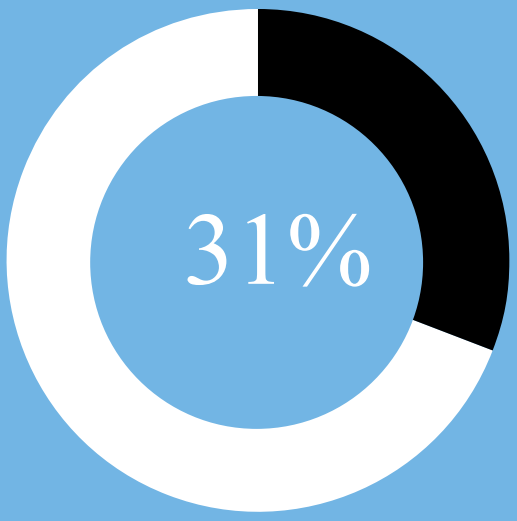
Cependant, le RGPD n'est pas uniquement un enjeu de cybersécurité. S'il vise la protection des données personnelles contre les attaques et les fuites, ce règlement concerne tout autant la manière dont les organisations recueillent, conservent, utilisent et divulguent ces données. En revanche, la Directive sur la sécurité des réseaux et des systèmes d'information (connue sous l'acronyme NIS- *Network and information system),* qui s'applique seulement aux « opérateurs de services essentiels », porte exclusivement sur la sécurité des réseaux - voir page 12).

Ainsi, les nouvelles règles du RGPD sont plus exigeantes à propos du consentement « sans équivoque » et « explicite » pour la collecte des données et élargiront, dans de nombreux cas, la définition des données personnelles en incluant des identifiants en ligne potentiels comme les adresses IP.

La gouvernance est un autre thème central, et les entreprises devront montrer que la protection des données est intégrée à leurs activités, en particulier, lors de conception de nouveaux produits, et qu'elles tiennent un registre des activités de traitement des données personnelles pour les sociétés de plus de 250 collaborateurs. En outre, les organisations dont l'activité exige un suivi régulier des personnes concernées et le traitement à grande échelle de données sensibles seront tenues de nommer un délégué à la protection des données *(Data Protection Officer,* DPO) devra rendre compte au plus haut niveau de l'organisation. Cette responsabilité pourra en pratique être partagée entre des personnes clés pour autant que l'on puisse identifier cette fonction.

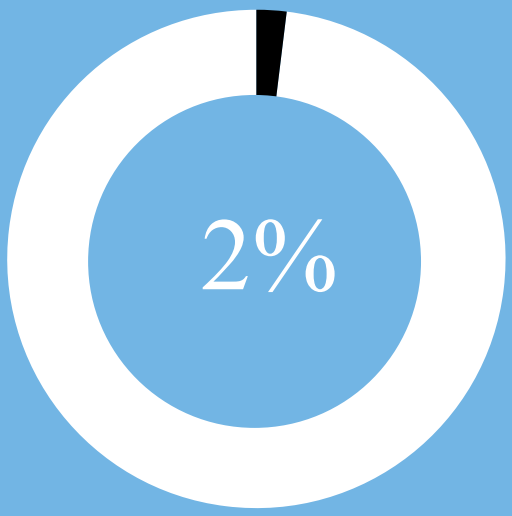
La portée géographique du RGPD constitue également un autre point critique. En effet, ce règlement ne s'applique pas seulement aux organisations situées à l'intérieur de l'Union européenne, mais également à celles qui proposent des biens ou des services aux personnes concernées de l'Union européenne, ou qui contrôlent leur comportement. Le transfert de données d'un pays à un autre est possible si les règles de protection des données des pays de destination sont au même niveau que le RGPD. Par exemple, les sociétés basées aux États-Unis peuvent utiliser le « bouclier vie privée UE-États-Unis », un cadre de référence pour les échanges de données personnelles qui a été jugé conforme à la nouvelle réglementation de l'Union européenne.

Votre organisation est-elle prête pour le RGPD ?



Seuls 31 % des décideurs considèrent que leur organisation est en conformité

Source : Veritas



Seules 2 % des organisations semblent être totalement en conformité avec le RGPD

Source : Veritas

« **La protection des données personnelles** est un domaine que nous **ciblons** en particulier, compte tenu du RGPD qui entrera en vigueur **l'année prochaine.** Les données et **la gestion des données** sont devenus des sujets prioritaires parce que la **gouvernance** des données et la **gestion** des données ne se limitent pas seulement à la sécurité et à la confidentialité – elles visent également les processus internes afin d'**optimiser,** de conserver les données, d'avoir conscience des données disponibles et de la manière dont elles sont utilisées et **gérées** à **but commercial** ».

Responsable de l'audit interne, fournisseur multinational de réseau mobile au Royaume-Uni

« Nous avons effectué des missions d'audit sur **l'état de préparation au RGPD** cette année, mais le sujet de la donnée – **la création, la protection, la gestion des données** – résulte en partie de la maturité et de la dépendance de notre organisation envers les données. Pour nous, c'est un domaine important et la nouvelle réglementation permet de mettre en exergue et de relancer le sujet. Nous l'avons partiellement examiné cette année et nous aborderons **plus globalement cette question de la donnée** l'année prochaine, compte tenu de notre dépendance à cet égard ».

Responsable de l'audit interne, société multinationale d'ingénierie et de production au Royaume-Uni

Les exigences de la Chine

Ce n'est pas seulement l'Union européenne qui s'intéresse à la protection des données. En juin 2017, la Chine a adopté sa propre loi qui vise à la fois la cybersécurité et la protection des données, fusionnant en substance les dispositions de la directive européenne sur la sécurité des réseaux et de l'information et le RGPD. À maints égards, la Loi sur la cybersécurité de la République populaire de Chine concorde avec le RGPD. Par exemple, pour ce qui est du consentement pour la collecte de données et la protection contre des pertes grâce au chiffrement. Cependant, il y a d'autres points d'attention majeures pour les multinationales, car les « infrastructures essentielles » comme les sociétés de services publics et les banques doivent conserver en Chine les informations personnelles recueillies dans le pays, ce qui pourrait nécessiter le rapatriement des données qui sont hébergées sur le *cloud* (ou « informatique en nuage ») à l'étranger. En outre, les sociétés devront se soumettre à un contrôle des régulateurs avant de transférer des quantités importantes de données personnelles à l'étranger. Toute organisation opérant en Chine et susceptible d'être exposée à des risques de non-conformité à cette réglementation devrait demander conseil à un expert juridique.

Du point de vue de l'audit interne

Les équipes juridiques et informatiques sont déjà en train d'aborder la conformité au RGPD et l'audit interne est bien placé pour donner une assurance sur la conformité de l'organisation. En menant une évaluation des risques descendante *(Top-down)* et en utilisant des techniques d'analyse des écarts pour revoir les systèmes de contrôle existants, l'audit interne peut identifier les domaines clés qui doivent être améliorés, et donner des conseils sur la mise en œuvre pratique des nouveaux systèmes de contrôle et processus.

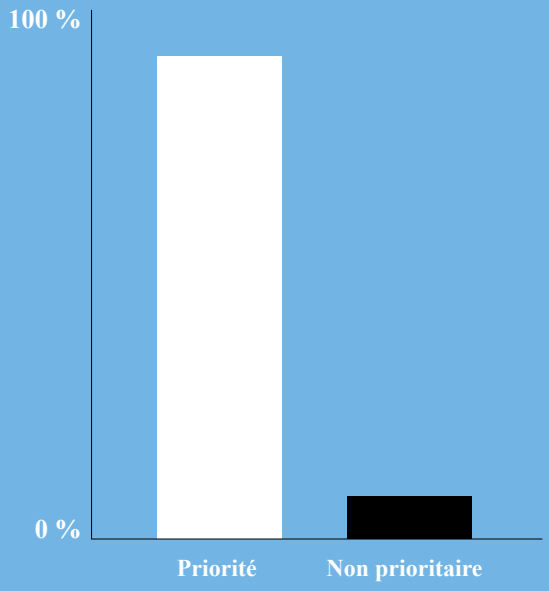
Questions clés :

- Une évaluation des risques a-t-elle été menée pour comprendre si l'organisation est en conformité et dans quels domaines des efforts restent à faire ?
- L'organisation a-t-elle cartographié ses données à caractère personnel (en les distinguant des autres données) ?
- Le cyber-périmètre de l'organisation est-il sécurisé et les données personnelles sont-elles protégées, sont-elles par exemple chiffrées ?
- L'organisation traite-t-elle des données personnelles sur une grande échelle, et le cas échéant, un DPO, interne ou externe, a -t-il été nommé ?
- Les prestataires d'assurance ont-ils accès à la fonction de DPO quelle que soit la manière dont elle est remplie ?
- Une procédure de reporting à l'autorité nationale compétente a-t-elle été mise en place pour être utilisée en cas de violation de données personnelles ?
- L'organisation a-t-elle défini un programme pour accroître la sensibilisation à la gestion, la sécurité et la divulgation de données personnelles et a-t-elle formé le personnel sur ces sujets ?
- Les principes concernant la protection des données ont-ils été inscrits dans les contrats avec les tiers ou les services de traitement de données concernés ?
- Des mesures sont-elles en place pour s'assurer que l'organisation demeure en conformité après le 25 mai 2018, y compris l'ajout d'une mission au plan d'audit 2018/2019 ?

Les sociétés américaines donnent la priorité au RGPD

92 % des sociétés américaines considèrent que la conformité avec le RGPD de l'Union européenne est une priorité absolue dans leur programme 2017 concernant la protection et la sécurité des données

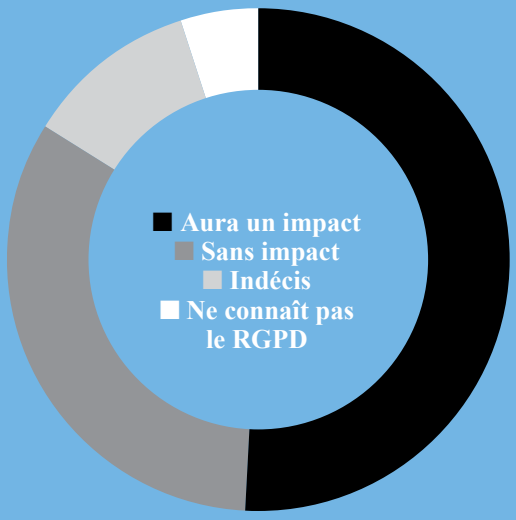
Source : PwC



Sensibilisation au RGPD

51 % des dirigeants et des professionnels de la sécurité des systèmes d'information considèrent que le RGPD aura un impact sur leurs sociétés, 33 % n'envisagent aucune incidence, 11 % sont incertains et 5 % ne connaissent pas bien le RGPD

Source : Imperva



« Le RGPD et ses **répercussions** ont une importance croissante. L'entreprise a **mis en place** une équipe **pluridisciplinaire** avec un soutien externe pour étudier l'évolution de notre position actuelle par rapport à celle où nous devrons être lorsque la **loi** entrera **en application**, ainsi que l'évolution ultérieure. En termes de missions d'assurance, le comité d'audit souhaite dans un premier temps que nous évaluions le dispositif lui-même, et qu'ensuite nous élaborions notre propre programme pour s'assurer régulièrement que l'organisation a mis en place les processus nécessaires afin de rester en conformité ».

Responsable de l'audit interne, groupe bancaire multinational de l'Euro Stoxx 50

CYBERSÉCURITÉ : LE CHEMIN DE LA MATURITÉ

L'attaque mondiale de Wannacry, dont on a considéré qu'elle avait infecté plus de deux millions d'ordinateurs dans plus de 150 pays, a mis l'accent sur la cyber-résilience et la sécurité de l'information en 2017.

En 24 heures, le cryptovirus, un type de rançongiciel auto-répliquant, a pris en otage les systèmes d'information d'organisations très importantes allant du National Health Service britannique à l'entreprise Telefónica en Espagne, FedEx et Deutsche Bahn, pour ne mentionner que celles-ci. Si les administrateurs portaient déjà une attention particulière à la cyber-assurance, Wannacry, et plus tard Peyta, une attaque mondiale qui l'a suivi de peu, ont hissé ce sujet en tête des priorités des comités d'audit pour 2017 et il demeurera une priorité majeure en 2018.

La cybersécurité s'est désormais imposée comme un risque clé pour l'organisation. L'information numérique s'est infiltrée pratiquement dans tous les aspects des opérations, indépendamment du secteur, des données clients à la propriété intellectuelle et aux dossiers RH. Cette tendance va aller en s'accentuant dans la mesure où les organisations exploitent l'internet des objets, font migrer de plus en d'opérations vers le *cloud* et passent à des modèles économiques dépendants des données et basés sur le numérique. Ceci signifie que pratiquement toutes les organisations sont exposées, à la fois aux cyber-criminels et aux pirates informatiques externes, mais également aux collaborateurs malveillants et aux employés négligents qui ne respectent pas les procédures.

Sensibilisation versus état de préparation

Il existe un écart persistant entre la sensibilisation des organisations aux cyber-risques et leur état de préparation pour résister à des attaques potentielles auxquelles il faut remédier. Alors que 62 % des organisations s'attendent à ce que les cyber-risques entraînent des bouleversements majeurs dans les trois prochaines années, 74 % ont une maturité très faible ou inexistante concernant les cyber-risques[3]. Il s'agit à l'évidence d'un sujet extrêmement préoccupant.

Ces dernières années, les gouvernements ont répondu à la menace croissante en lançant des centres d'expertise, comme le Centre national de cybersécurité au Royaume-Uni et le Centre national de cryptologie en Espagne, ou l'Agence nationale de la sécurité des systèmes d'information en France pour défendre les systèmes des administrations publiques et alerter le secteur privé de menaces émergentes. Des organismes européens publics (comme l'ENISA- l'Agence européenne chargée de la sécurité des réseaux et de l'information) et privés (comme l'Organisation européenne pour la cybersécurité) ont également été créés pour promouvoir les cyber-innovations et les meilleures pratiques.

En outre, les lignes directrices gouvernementales et les programmes de certification sont un bon point de départ pour les organisations afin de se protéger contre les vulnérabilités. Ils donnent à l'audit interne des fondements pour apporter une assurance essentielle au Conseil. Par exemple, désormais toutes les organisations au Royaume-Uni auraient dû faire l'objet d'une évaluation Cyber Essentials Plus, et même si celle-ci n'est offerte qu'aux organisations basées au Royaume-Uni, toutes les organisations devraient tout au moins avoir adopté les cinq contrôles clés de ce plan (voir page 13). De même l'ANSSI publie régulièrement des recommandations : (https://www.ssi.gouv.fr/entreprise/actualite/adoptez-les-bonnes-pratiques-de-linformatique-et-devenez-acteur-de-la-securite-du-numerique/)

Une fois que l'essentiel est traité, les organisations ont le choix d'adopter des guides et des cadres de référence, comme ceux proposés par le NIST pour l'amélioration de la cybersécurité des infrastructures critiques *(NIST Framework for Improving Critical Infractstructure Cybersecurity)*, COBIT 5 de l'ISACA et l'*Emerging Cyber Nexus,* le *SANS Institute,* les 20 Contrôles critiques de sécurité et la liste de contrôles pour la conformité à la norme PCI DSS. De même, les fonctions d'audit interne devraient consulter le guide d'audit GTAG « Évaluer le risque de cybersécurité : les rôles des trois lignes de maîtrise » de l'IIA-*The Institute of Internal Auditors* pour des lignes directrices sur la manière dont elles peuvent apporter de la valeur ajoutée par leur mission d'assurance.

Il est essentiel de mettre en place des contrôles élémentaires, d'adopter un cadre de référence adapté à l'organisation et de positionner l'audit interne pour qu'il évalue l'efficacité de ces mesures initiales, afin d'atteindre un niveau minimal de maturité vis-à-vis des cyber-risques.

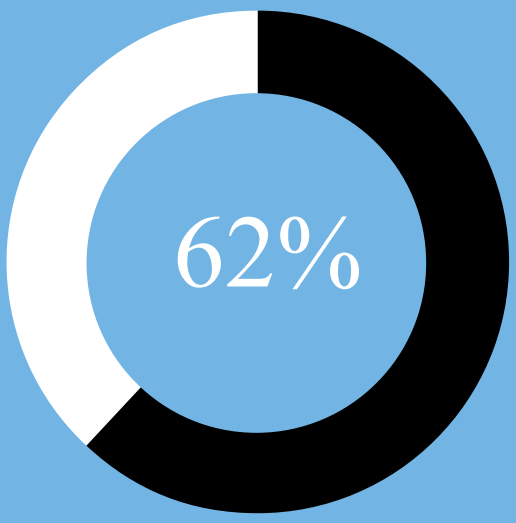
La cyber-culture

Les organisations ont tendance à envisager la cybersécurité à travers un prisme technologique en investissant dans les derniers outils de sécurité, puis en s'assurant que ceux-ci fonctionnent et que les systèmes de contrôle et les procédures sont suffisants. Cependant, alors que le fonctionnement de logiciels et de technologies correctement configurés et maintenus est relativement prévisible, on ne peut pas en dire autant du comportement des utilisateurs. Des données critiques peuvent être compromises ou perdues à cause de la négligence de collaborateurs. Il est par conséquent crucial que – en plus des systèmes de contrôle et des défenses techniques comme les pare-feu – les organisations intègrent une cyber-culture qui se manifeste dans le comportement du personnel et est mise en pratique grâce à des programmes de formation et de sensibilisation dans toute l'entreprise.

« Nous avons effectué des missions d'audit concernant **les cyber-menaces,** la perte de données, la sécurité des réseaux, les appareils mobiles et ainsi de suite depuis trois - quatre ans, et c'est un domaine auquel nous devons accorder plus d'importance. Contrairement aux risques opérationnels plus traditionnels, les technologies sont **en évolution constante,** être à l'équilibre ne suffit donc pas pour préparer le futur. Nous devons suivre ce qui change afin que notre **situation ne s'érode pas** ».

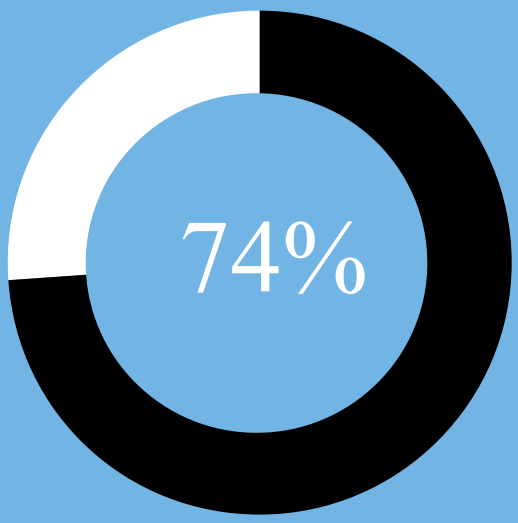
Responsable de l'audit interne, groupe de construction et d'infrastructure multinational espagnol

L'écart entre la cyber-sensibilisation et l'état de préparation persiste



62 % des organisations s'attendent à ce que les cyber-risques entraînent des bouleversements majeurs dans les trois prochaines années

Source : PwC



Pourtant 74 % des organisations ont une maturité faible ou inexistante concernant les cyber-risques

Source : PwC

« **Les gens parlent de « disruptions » numériques et d'innovation** et de leurs impacts, mais **font-ils toujours ce qu'ils devraient faire concernant les systèmes existants ?** Ce qui s'est passé avec l'attaque mondiale de **Wannacry** montre ce qui peut arriver quand les organisations oublient toutes les portes qu'elles ont laissé ouvertes. Nous sommes en train de créer **un service d'audit spécialisé en système d'information,** de rassembler nos collaborateurs qui ont des **compétences dans ce domaine,** et de chercher **à améliorer notre offre** ».

Administrateur, agence gouvernementale du Royaume-Uni

Tous les collaborateurs, y compris les prestataires ou ceux qui travaillent à distance, doivent comprendre exactement ce qu'il est attendu d'eux en termes de procédures et de comportements. Cette réponse de l'organisation est une des étapes essentielles pour atténuer les cyber-risques et les risques concernant la vulnérabilité des systèmes d'information. Dans ce contexte, l'audit interne peut jouer un rôle créateur de valeur en donnant l'assurance que, non seulement le cyber-contrôle est en place et fonctionne, mais que la sensibilisation aux cyber-risques est élevée et que les meilleures pratiques se reflètent dans les comportements des collaborateurs.

La cyber-conformité

En plus du besoin de protéger des informations créatrices de valeur et la réputation de l'organisation, il y a une composante conformité à prendre en considération. Nous avons consacré un thème au RGPD (voir page 6) parce qu'il s'appliquera à toutes les organisations et qu'il vise spécifiquement les données personnelles.

La directive sur la sécurité des réseaux et des systèmes d'informations (SRI), qui devra être transposée dans les législations nationales d'ici le 9 mai, attire moins l'attention. Elle s'applique aux « opérateurs de services essentiels » à la fois dans le secteur privé et le secteur public, vise davantage la sécurité des réseaux et la continuité des services. Contrairement au RGPD, les amendes ne concernent pas les violations de données mais les manquements de signalement d'un piratage informatique.

La première étape pour toutes les organisations est de déterminer si elles relèvent du champ d'application de cette directive, qui s'applique dans les secteurs de l'énergie, des transports, des infrastructures bancaires et des marchés financiers, de la santé, de l'eau, dans certains domaines de l'administration publique et à certains fournisseurs de services numériques. Les opérateurs concernés devront prendre des mesures de sécurité adéquates pour empêcher les vulnérabilités dans les réseaux, garantir la sécurité des réseaux et des systèmes d'information et gérer les incidents, y compris en signalant tout incident grave à l'autorité compétente. Les organisations devront échanger avec l'autorité nationale pour déterminer ce qui constitue un incident grave.

L'audit interne a un rôle à jouer auprès du Conseil en lui donnant l'assurance que l'organisation a déterminé si elle est visée par la directive et qu'elle a mis en place des mesures et des procédures pour respecter les nouvelles règles, en renforçant les réseaux et en mettant en place des procédures adéquates de reporting.

Du point de vue de l'audit interne

Tous les conseils devraient, avec l'aide de l'audit interne, avoir une vue d'ensemble des réponses de l'organisation à la cyber-menace croissante, ainsi que de la qualité de sa cyber-gouvernance et de son management des risques. Au fur et à mesure, les travaux d'assurance pourront approfondir des domaines spécifiques tels que, par exemple, la cartographie des données et des points d'entrée du réseau, la robustesse de la gestion des droits d'accès, des tests de pénétration du réseau, des missions d'audit des tiers prestataires de services informatiques dans le *cloud*, l'assurance que les plans de secours et de remédiation sont suffisants, et l'évaluation de la capacité de l'organisation à répondre à cette menace en constante évolution.

Questions clés :

- L'organisation a-t-elle reconnu la menace potentielle que représentent les cyber-risques envers la résilience de ses activités, sa réputation et ses résultats ?
- Les contrôles clés sont-ils en place ou un cadre de référence reconnu a-t-il été mis en œuvre ?
- L'organisation a-t-elle compris quelles sont ses données les plus créatrices de valeur et ont-elles été cartographiées ?
- L'organisation a-t-elle mis en place des pare-feu et des protections efficaces et à jour contre les programmes malveillants ?
- Les protections existantes ont-elles été soumises à des tests efficaces de pénétration ?
- La gouvernance des droits d'accès est-elle suffisamment robuste ?
- La direction des systèmes d'information ou la cyber-fonction dédiée se tient-elle au courant des nouvelles menaces et des cyber-attaques émergentes ?
- A-t-on instauré une véritable cyber-culture et les politiques se reflètent-elles dans le comportement des collaborateurs ?
- Les fonctions d'assurance ont-elles des compétences techniques suffisantes pour interpréter leurs constats ?
- L'organisation est-elle prête à réagir et à se rétablir dans le cas probable d'une attaque ?

« C’est une préoccupation majeure parce que ce risque reste inconnu. Le **niveau de maturité** de l’organisation pour l’atténuer et le surveiller **exige encore l’attention du Conseil,** du comité des risques et de la direction générale. Ensuite, il y a la maturité technique, les équipes et les compétences. C’est **le point d’attention de l’audit interne.** Nous remodelons et faisons évoluer notre profil de compétences, en recrutant des experts en la matière et en définissant un **programme d’audit élémentaire de la cybersécurité.** Nous pensons que la plupart des organisations de notre secteur sont dans la même situation ».

Responsable de l’audit interne, groupe bancaire multinational espagnol

Les 5 fondamentaux de la cybersécurité

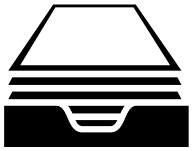
1 Pare-feu à la frontière et passerelles Internet
La première étape consiste à cartographier et à protéger votre périmètre. Les pare-feu et les passerelles offrent un niveau de protection élémentaire quand un utilisateur se connecte à Internet et empêchent les attaquants ou les menaces extérieures d’avoir accès au réseau de l’organisation en surveillant tout le trafic et en bloquant les incidents à l’entrée, ainsi qu’en empêchant les collaborateurs d’accéder à des zones du réseau pour lesquelles ils n’ont pas d’autorisation.

2 Configuration sécurisée
Les pare-feu et les passerelles ne sont d’aucune utilité s’ils ne sont pas correctement configurés. Des agents mal intentionnés peuvent utiliser des outils courants d’analyse de la sécurité pour déceler facilement les vulnérabilités du réseau, qui peuvent alors être exploitées, avec pour conséquence un système compromis et une perte de données.

3 Contrôle des accès
Il est important de restreindre les accès au minimum et d’éviter ce que l’on pourrait appeler une « dérive des accès ». Les comptes utilisateurs, particulièrement ceux avec des droits d’accès spéciaux ne devraient être attribués qu’aux personnes autorisées ; ils doivent être gérés efficacement et donner le niveau minimum d’accès aux applications, ordinateurs et réseaux. Il convient également d’utiliser des identifiants uniques et de changer régulièrement les mots de passe. Les droits d’accès devraient être revus régulièrement.

4 Protection contre les programmes malveillants
Il est important de protéger l’organisation contre des logiciels malveillants qui chercheront à accéder aux dossiers stockés sur le réseau. Une fois installé, un programme malveillant peut accéder à des informations confidentielles et les voler, endommager des fichiers ou les verrouiller et les garder contre rançon. La protection contre les programmes malveillants permet d’identifier et d’empêcher ou supprimer toutes les menaces potentielles venant d’un logiciel malveillant. De tels logiciels de protection doivent être mis à jour régulièrement et installés sur tous les appareils connectés.

5 Gestion des *patchs*
Les cyber-criminels exploitent souvent des vulnérabilités bien connues dans les logiciels ou les systèmes d’exploitation pour obtenir un accès. La gestion des *patchs* est le fait de maintenir à jour les logiciels sur les ordinateurs et les périphériques du réseau pour qu’ils soient capables de résister à des incidents. Les *patchs* (correctifs) de mise à jour et de sécurité devaient être installés rapidement et tout logiciel non pris en charge ou sans licence devrait être supprimé.



COMPLEXITÉ RÉGLEMENTAIRE ET INCERTITUDE

En se projetant en 2018 et au-delà, la charge de la mise en conformité des organisations peut sembler intimidante. Pratiquement tous les responsables de l'audit interne citent le RGPD comme un domaine qui demande leur attention et c'est d'ailleurs pourquoi nous avons consacré une rubrique à ce règlement imminent et d'une grande portée. Mais d'autres problématiques réglementaires sont sur la liste des priorités des organisations.

Les secteurs très réglementés comme les services publics et les télécommunications doivent tenir compte de réglementations spécifiques en Europe, mais ce sont les établissements financiers qui seront les plus touchés par des réformes imminentes.

MiFID II

Dans le secteur financier, la plus grande évolution législative depuis plus d'une décennie doit avoir lieu le 3 janvier 2018. L'objectif de la deuxième directive sur les marchés d'instruments financiers, plus connue sous le nom de MiFID II, est de renforcer la protection des investisseurs, d'empêcher les abus de marché et d'accroître la transparence des transactions sur les produits d'investissement comme les actions, les obligations et les *swaps*, et concerne autant de sujets que les transactions électroniques, le reporting et le stockage d'informations. Les changements requis nécessitent également des travaux sur la manière dont l'environnement de contrôle de l'organisation doit changer pour maintenir la conformité après l'entrée en vigueur de cette réglementation.

Sa mise en œuvre a dû être retardée d'une année parce que les établissements et les régulateurs devaient encore mettre des systèmes en place pour s'y conformer. Pas plus tard qu'en juillet 2017, une étude a montré que 90 % des investisseurs institutionnels en Europe risquent de ne pas être en conformité, et qu'ils étaient mal préparés et débordés dans leurs travaux de mise en conformité[4]. De plus, mi-2017, un tiers des règles restaient encore à formaliser par les régulateurs nationaux ou par des lignes directrices techniques détaillant exactement la manière dont elles devraient être mises en application.

Conflit entre les exigences de conformité

La situation est encore plus compliquée par l'incompatibilité apparente entre MiFID II et le RGPD. Selon la première, toutes les communications téléphoniques, tous les courriels et toutes les autres communications électroniques qui sont censés avoir pour résultat des opérations et des transactions doivent être enregistrés. Parallèlement, le RGPD impose des règles

Normes comptables imminentes

2018 verra l'introduction de deux nouvelles normes IFRS et l'application anticipée de la norme IFRS 17.

IFRS 9 Instruments financiers exige qu'une entité reconnaisse, à sa juste valeur, un actif ou un passif financier lié aux dispositions contractuelles de l'instrument dans ses états financiers.

IFRS 15 Produits des activités ordinaires tirés de contrats conclus avec des clients établit les principes à appliquer par une entité lors de la transmission des informations concernant la nature, le montant, le calendrier et le degré d'incertitude des produits tirés d'un contrat conclu avec un client.

IFRS 17 Contrats d'assurance communique des informations qui montrent l'effet que les contrats d'assurance ont sur la situation financière, la performance financière et les flux de trésorerie d'une entité.

Pour plus d'informations, veuillez consulter www.ifrs.org

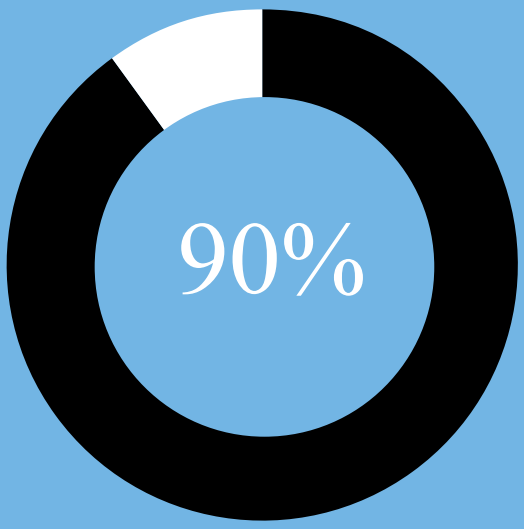
« Il y a des **contradictions** entre ce que les **régulateurs locaux** disent et ce que la **Banque centrale européenne** exige pour l'ensemble du groupe. Ceci affecte les multinationales et c'est un véritable casse-tête pour nous. Il est difficile de savoir **comment répondre à de nombreux régulateurs** tout en étant une entreprise profitable et bien organisée. Ceci a encouragé le dialogue avec les régulateurs ».

Responsable de l'audit interne, groupe bancaire multinational espagnol

« Les sujets réglementaires liés au **Brexit** en termes de localisation de certains types d'activité et d'autorité de **régulation** sont considérables. Face au rythme incessant, à l'échelle et à **la complexité des modifications de la réglementation,** notre équipe de gestion des risques émergents doit jouer le rôle d'une tour de contrôle et comprendre ce sur quoi l'organisation doit se concentrer – que ce soit des **évolutions de systèmes, de processus ou de reporting** exigées par les régulateurs et notre capacité **à mener ces changements à bon port** en temps voulu ».

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

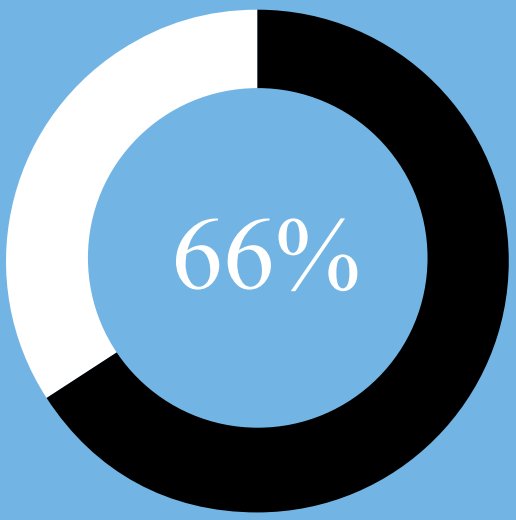
Se préparer pour MiFID II



90 % des investisseurs institutionnels en Europe risquent de ne pas être en conformité avec MiFID II

Source : PwC

Les risques d'un contrôle réglementaire approfondi



Les évolutions réglementaires et une surveillance réglementaire accrue sont vus comme des risques qui peuvent avoir un impact significatif pour 66 % des administrateurs

Source : PwC

beaucoup plus strictes de protection des données sensibles recueillies par tous les moyens d'enregistrement, avec des sanctions potentielles énormes en cas de violations. En renforçant le droit des personnes à ne pas accepter que leurs données soient recueillies lors d'appels téléphoniques et par d'autres moyens, le RGPD semble contredire l'interprétation des exigences de MiFID II.

Si des exceptions à cette collecte discrétionnaire des données peuvent être faites dans le cadre de MiFID II, les établissements financiers restent toujours exposés aux risques de violation des données s'ils n'arrivent pas à protéger de manière adéquate toute la nouvelle série de données personnelles qu'ils collecteront.

Janvier 2018 correspond également à l'entrée en vigueur de la directive sur les services de paiement II (DSP2), qui, en même temps qu'elle met fin aux surcoûts sur les cartes de crédit, est conçue pour accroître la concurrence en abaissant les barrières à l'entrée pour les startups de la Fintech. Ainsi, les banques, qui auraient l'avantage indu d'avoir une avance de plusieurs décennies sur les Fintech, auront l'obligation de donner aux autres organisations l'accès aux informations financières de leurs clients. Une fois de plus, ceci est perçu comme étant en contradiction avec les mesures de protection des données du RGPD. DSP2 signifie qu'il est probable que les banques partageront les données sur leurs clients avec des dizaines de sociétés Fintech. Alors que le RGPD vise à assurer la traçabilité, la sécurité et la suppression aisée des données des clients. Réconcilier ces deux obligations sera un véritable défi.

Devoir personnel de rendre compte

Au Royaume-Uni, les établissements financiers sont contraints de respecter le plan *Senior Managers and Certification Regime* (SM&CR), qui a été introduit dans le secteur bancaire en 2016. En 2017, la *Financial Conduct Authority* (FCA) a étendu ces règles à l'ensemble des établissements financiers et la cible devrait être élargie à compter de 2018. L'ensemble des collaborateurs seront concernés par le respect des règles d'intégrité, de conscience professionnelle, de compétence et de diligence. Ils devront également être transparents et coopérer avec les régulateurs, être attentifs aux intérêts des clients en les traitant équitablement et observer des règles adéquates de conduite des affaires. La FCA a lancé une consultation publique, pour un recueil des commentaires à ce sujet, jusqu'au 3 novembre 2017.

L'aspect le plus crucial du SM&CR est qu'il introduit le devoir de rendre compte pour les cadres dirigeants, ainsi, ils peuvent être tenus personnellement responsables de défaillances intervenues dans leur périmètre d'activité. Ces règles s'appliquent à tous les établissements qui ont des activités au Royaume-Uni, y compris les établissements étrangers qui ont une seule succursale dans ce pays.

Avec autant de changements en cours, il n'est guère étonnant que les fonctions de conformité soient sous pression. Le volume et le rythme des évolutions réglementaires sont une inquiétude majeure non seulement pour les professionnels de la conformité dans le secteur des établissements financiers, mais également pour leurs conseils. Des études montrent que ce sujet est prioritaire par rapport à la cyber-résilience et à la résilience face à l'évolution des technologies. Tous secteurs confondus, les évolutions réglementaires et la surveillance réglementaire accrue sont vus comme des risques ayant un impact significatif par 66 % des administrateurs et des cadres dirigeants[5]. Les conseils et les comités d'audit vont probablement souhaiter avoir l'assurance que la conformité est gérée avec efficacité.

Du point de vue de l'audit interne

La conformité et les risques réglementaires sont une préoccupation constante des organisations. Mais avec autant de changements majeurs se profilant à l'horizon ou ayant été récemment introduits, il y a plus que jamais une pression pour s'assurer que la conformité est gérée avec efficacité. Dans ce contexte, le référendum sur le Brexit et l'élection du président des États-Unis augmentent, pour d'innombrables organisations, les incertitudes en matière de réglementation particulièrement en ce qui concerne les échanges commerciaux. L'audit interne a un rôle à jouer pour évaluer si :

- les fonctions de conformité maîtrisent les dernières réglementations applicables,
- les mesures adéquates ont été prises pour s'assurer que l'organisation est en conformité ;
- le cas échéant, un dialogue avec les régulateurs concernés a été établi pour résoudre d'éventuelles incertitudes ou conflits avec des règles existantes ou à venir.

Questions clés :

- L'organisation a-t-elle l'assurance que tout ce qui est en son pouvoir est fait pour être en conformité avec toutes les réglementations pertinentes ?
- Des systèmes et des procédures de signalement des incidents de non-conformité et des moyens de dissuasion disciplinaires pour éviter que ceux-ci se produisent ont-ils été mis en place ?
- L'organisation revoit-elle les non-conformités et prend-elle des mesures pour s'assurer qu'elles ne se reproduisent pas ?
- La fonction de conformité a-t-elle des ressources adéquates et est-elle capable de recenser, prioriser et mettre en œuvre efficacement les réglementations à venir ?
- Des programmes de formation ont-ils été mis en place pour s'assurer que les collaborateurs et les autres représentants de l'organisation ont connaissance de leurs responsabilités en matière de conformité ?
- Si l'organisation est une multinationale, a-t-elle identifié des conflits entre les réglementations de différentes juridictions ? Les éventuels écarts irréconciliables ont-ils été signalés au régulateur concerné ?
- L'organisation est-elle suffisamment souple et modulable pour rester en conformité totale tout en se développant ?

Planification fiscale

En août 2016, l'Union européenne a condamné Apple à payer une somme record de 13 milliards d'euros d'impôts rétroactifs à l'Irlande après qu'il a été jugé qu'un accord entre la plus grande entreprise mondiale et l'administration fiscale irlandaise représentait une subvention publique illégale. Dans le cadre de cet accord, le taux d'imposition d'Apple n'était que de 0,5 % au lieu du taux de l'impôt sur les sociétés de ce pays qui est de 12,5 %.

En enregistrant ses profits au siège social irlandais, l'entreprise a évité de payer des impôts sur pratiquement tous les profits faits sur les milliards d'euros de produits vendus dans tout le marché unique de l'Union européenne. Apple et l'Irlande ont fait appel de cette décision, la résolution de cet appel prendra des années. Si la Commission européenne gagne, elle deviendra l'arbitre ultime de la fiscalité en Europe et ces décisions prévaudront sur les politiques nationales.

La décision et l'amende concernant Apple sont arrivées à point nommé. Un mois auparavant, l'Union européenne avait introduit la directive sur la lutte contre l'évasion fiscale (ATAD), qui avait précisément pour objectif d'empêcher l'exploitation de ces disparités fiscales entre les États membres. Moins d'une année plus tard, en mai 2017, ATAD II était introduit, étendant le traitement des disparités entre les États membres et les pays qui ne sont pas dans l'Union européenne. Ces nouvelles règles entreront en vigueur le 1er janvier 2020.

Le cadre de référence BEPS *(Base Erosion and Profit Shifting)* sur l'érosion de la base d'imposition et le transfert des bénéfices, publié en décembre 2015 par l'OCDE, a largement servi de référence à cette directive. Jusqu'à présent, plus de 100 pays ont édicté des règles sur la mise en œuvre de ces exigences en matière de reporting, qui ont été énoncées pour créer un système fiscal international plus équitable et plus efficace, comprenant des efforts croissants pour combler les lacunes, améliorer la transparence et s'assurer que les entreprises multinationales paient leurs impôts là où elles exercent effectivement leurs activités.

Il est peu probable que la planification fiscale disparaisse de la liste des priorités dans un futur proche, le public et les gouvernements nationaux accordant une grande attention à la manière dont les organisations traitent cette problématique. 91 % des multinationales considèrent que les bases d'imposition sont soumises à un examen plus approfondi de la part des autorités par rapport à l'an dernier. Ceci dit, 86 % des multinationales disent que leur organisation a évalué l'impact potentiel des changements liés au BEPS[6].

Cependant, l'incertitude politique qui se profile avec des questions comme le Brexit, la stabilité future de l'Union européenne et la nouvelle administration américaine, exige une attention particulière aux réformes fiscales potentielles et à leur impact sur les décisions stratégiques.

De nombreux conseils chercheront à comprendre comment le cadre de référence BEPS affecte les opérations de l'organisation et les processus de reporting financier, et les mesures à prendre face aux évolutions des politiques nationales provoquées par l'initiative BEPS. Dans certains cas, une demande de missions d'assurance concernant l'alignement des stratégies de planification fiscale avec les objectifs stratégiques et l'image de l'organisation, ainsi qu'à propos des plans d'urgence face à une controverse qui nuirait à la réputation de l'organisation.

« **Les aspects réglementaires** changent souvent et sont très **complexes**, par exemple les exigences de l'Union européenne en matière de dégroupage des activités de vente et de distribution d'énergie dans le cadre du « troisième paquet » législatif. Cette réglementation a eu comme résultante la création d'une organisation ad hoc pour la vente et d'une autre pour la distribution. **Le plan d'audit doit comporter des marges de manœuvre** au fil de l'évolution des lois et règlements.
Le plan doit être suffisamment flexible pour que l'audit interne puisse répondre aux requêtes du régulateur ».

Responsable de l'audit interne, groupe polyvalent de services publics italien

RYTHME DE L'INNOVATION

De plus en plus, les leaders du marché doivent réfléchir comme des startups afin de défendre leurs positions sur les marchés et d'être à la pointe de l'innovation. En un peu plus d'une décennie (entre 2005 et 2016), les dépenses mondiales de R&D ont eu un taux annuel de croissance de 4,94 % pour atteindre 680 milliards de dollars US[7]. En effet, les organisations ont cherché à augmenter leur chiffre d'affaires grâce à l'innovation à une époque où les avancées technologiques se poursuivent à un rythme soutenu.

L'accent est principalement mis sur la transformation des entreprises de la vieille économie analogique en acteurs numériques agiles qui tirent profit de l'optimisation du back-office et de l'efficience liée à l'automatisation tout en maîtrisant le Big Data (ou les « mégadonnées ») pour obtenir un avantage compétitif. Les banques investissent massivement dans les Fintech pour faire évoluer leurs modèles économiques basés sur des agences et devenir des opérateurs numériques plus compétitifs à l'ère des technologies blockchain. Les distributeurs explorent les applications de réalité virtuelle et l'utilisation de drones pour améliorer l'expérience client. Des organisations, surtout dans l'industrie, utilisent l'internet des objets pour rendre leurs opérations plus efficaces et réaliser des gains d'efficacité. Avec les voitures autonomes, les constructeurs automobiles ressemblent de plus en plus à des entreprises de logiciels et de technologie.

« Il est très difficile de créer des organisations innovantes qui peuvent **concurrencer les Fintech** créées dans les 12 à 24 derniers mois. Nous sommes une banque multinationale et nous avons existons **depuis plus d'un siècle.** Du point de vue des risques, l'audit interne doit être **vigilant sur la manière dont l'organisation innove.** Tout le monde veut **créer des lacs de données et utiliser la blockchain,** mais peu réfléchissent à des **référentiels adaptés à la gestion des risques** liés à ces activités. Il est illusoire de vouloir gérer l'innovation avec d'anciens cadres qui **limiteraient l'idée même d'innovation.** C'est désormais un véritable défi pour l'audit interne ».

Responsable de l'audit interne, groupe bancaire multinational espagnol

Ce rythme rapide d'innovation n'est pas naturel pour des organisations bien établies, qui évoluent lentement. Les startups peuvent prospérer en créant des environnements dans lesquels la rapidité, l'expérimentation, l'échec et l'apprentissage rapide font partie du fonctionnement de leur organisation. En contraste, dans les grandes organisations, des référentiels de gestion des risques ont été soigneusement établis et le changement y est intentionnellement graduel.

Des environnements qui évoluent aussi lentement peuvent asphyxier l'innovation et exposer les opérateurs installés sur le marché à des révolutions numériques. Un administrateur sur trois indique un bouleversement de modèle économique dans les cinq prochaines années[8]. De toute évidence, devenir obsolète est un risque stratégique important que les organisations doivent atténuer ; dans le même temps, se précipiter la tête la première dans une nouvelle direction et investir massivement présentent également des risques inhérents d'échec. Les décisions d'investissement doivent être les plus efficaces possibles pour financer et allouer les ressources aux projets les mieux adaptés, leur retour sur investissement (ROI) doit être correctement analysé et il convient de savoir tirer un trait sur des innovations sans intérêt.

En outre, les démarches d'innovation deviennent plus complexes. Jusque-là, les services internes de R&D étaient les seuls responsables de cette activité. Désormais, les multinationales testent l'esprit entrepreneurial de la Silicon Valley en mettant en place leurs propres filiales de capital-risque d'entreprise et des incubateurs de startups. Encore plus récemment, il est question de coopétition, c'est-à-dire de stratégies d'innovation ouverte dans lesquelles des organisations, et dans certains cas des concurrents, coopèrent dans leur intérêt mutuel et pour faire progresser leurs secteurs. Selon les projections, au cours de la prochaine décennie, les modèles internes diminueront de 23 % et les réseaux de collaboration augmenteront de 50 %[9]. Tous ces modèles soulèvent des questions sur la gestion des risques.

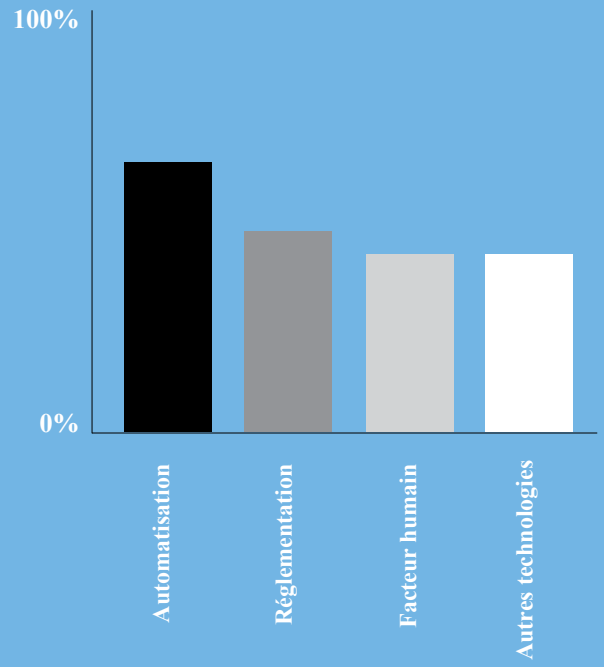
Big Data, méga risques

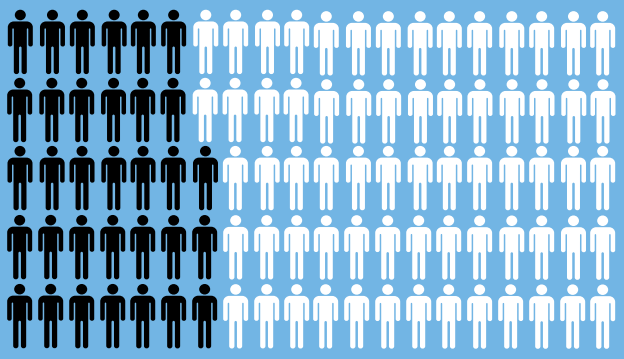
Ces dernières années, l'un des termes qui est sur toutes les lèvres dans le monde des affaires est le Big Data. Comme nous sommes plus nombreux à être connectés à Internet et que nous le faisons pendant plus longtemps, laissant une traînée de données partout où nous allons, les organisations ont des possibilités pratiquement illimitées d'obtenir des renseignements. Les données sont devenues essentielles

Les principaux facteurs de bouleversement pour les organisations

51 % des dirigeants disent que l'automatisation sera le principal facteur de bouleversement d'ici 25 ans, suivi par la réglementation (43 %), le facteur humain (38 %) et d'autres technologies qui ne sont pas encore disponibles (38 %)

Source : Thomson Reuters





Un tiers des administrateurs considèrent que leur modèle économique sera bouleversé dans les cinq prochaines années

Source : McKinsey

« Il y a une série de nouveaux **risques** mondiaux liés à la **transformation** de l'**économie**. Le **monde numérique remplace** de plus en plus le monde physique et le rythme de **l'innovation**, de la numérisation et **du commerce électronique** est rapide et **change constamment.** Il y a par conséquent de nombreuses évolutions de systèmes, **de processus, des contrôles** et des risques eux-mêmes.
Le recours à des tiers pour de **nouveaux types d'opérations,** comme la logistique, entraîne dans notre cas des **risques significatifs** ».

Responsable de l'audit interne, entreprise néerlandaise multinationale du secteur du vêtement

« Ce monde évolue constamment et le **rythme du changement s'accélère,** ce qui met la **pression sur les organisations pour qu'elles s'adaptent** afin de perdurer. Les organisations essaient peut-être de faire trop de changements simultanément et ne sont pas vraiment capables de maîtriser tout ce à quoi elles tentent de parvenir. Ceci rend difficile la réconciliation entre les objectifs que l'organisation a fixés et les **priorités changeantes** qu'elle a. Quand il y a une crise, on se bouscule pour éteindre les incendies, pendant ce temps 20 feux supplémentaires s'allument derrière soi. On peut considérer qu'il s'agit d'une **ambition excessive** de la part d'organisations qui **essaient de traiter tout en même temps** et qui, ce faisant, s'exposent elles-mêmes à des risques ».

Responsable de l'audit interne, groupe multinational espagnol fournisseur de prestations informatiques

pour comprendre les comportements des clients et les entreprises cherchent à exploiter les données pour prévoir les ventes futures et avoir un marketing précisément ciblé pour parvenir à des taux de transformation plus élevés.

Le chiffre d'affaires mondial pour le Big Data et l'analyse de données commerciales passera de 130,1 milliards de dollars en 2016 à plus de 203 milliards de dollars en 2020, soit un taux annuel de croissance égal à 11,7 %. Le secteur bancaire est celui qui investit le plus dans le Big Data et l'analyse de données commerciales (environ 17 milliards de dollars en 2016). C'est également celui qui connaîtra la plus forte hausse de dépenses[10].

Malgré tout, une des critiques que l'on peut faire aux organisations qui se précipitent pour exploiter le Big Data est leur incapacité à se demander « pourquoi ? » avant de se demander « comment ? ».

Beaucoup d'entreprises ont obtenu des informations sur leurs activités et leurs clients qui, en soi, n'ont pas de valeur intrinsèque et ne leur permettront pas d'accroître leur chiffre d'affaires. De plus, de nombreux projets concernant le Big Data n'ont pas de ROI tangible déterminé à l'avance.

La progression rapide des lacs de données analysables et d'autres projets liés au Big Data est relativement nouvelle. Cependant, les changements opérationnels ne sont pas toujours effectifs. Or, les innovations vont de concert avec une incertitude et des risques, et pour réagir aux évolutions dans l'environnement (que ces évolutions soient numériques ou non) et augmenter le chiffre d'affaires, il convient d'assurer la gestion du changement au niveau des procédures, des processus, des opérations et des systèmes.

Du point de vue de l'audit interne

Les technologies évoluent rapidement et les organisations doivent surfer sur la vague de l'innovation pour ne pas perdre de terrain. Cela met la pression sur l'audit interne pour s'assurer que la réflexion de la direction générale en matière d'investissements dans de nouvelles technologies, de nouveaux modèles économiques et de nouvelles approches organisationnelles est solide et se traduit par un ROI. Les organisations devraient avoir mis en place des procédures d'analyse prospective pour identifier les menaces et les opportunités technologiques, et l'audit interne peut jouer un rôle dans l'évaluation de la qualité de cette collecte de renseignements.

Les projets de R&D et d'innovation devraient être audités pour s'assurer qu'ils sont gérés efficacement afin d'atténuer les risques liés aux projets et, à l'approche de leur déploiement opérationnel, traiter les risques liés à leur exécution. Dans le même temps, l'audit interne doit trouver le juste équilibre pour ne pas ralentir ou faire obstacle aux innovations rapides qui seront cruciales pour le succès de l'organisation dans le futur, mais également en donnant l'assurance que ces projets apporteront les avantages promis. La numérisation a aussi une incidence sur l'environnement de contrôle, ce qui pourrait augmenter la probabilité de fraudes et par conséquent renouveler l'attention que l'audit interne porte sur des dispositifs de contrôle élémentaires comme la séparation des fonctions.

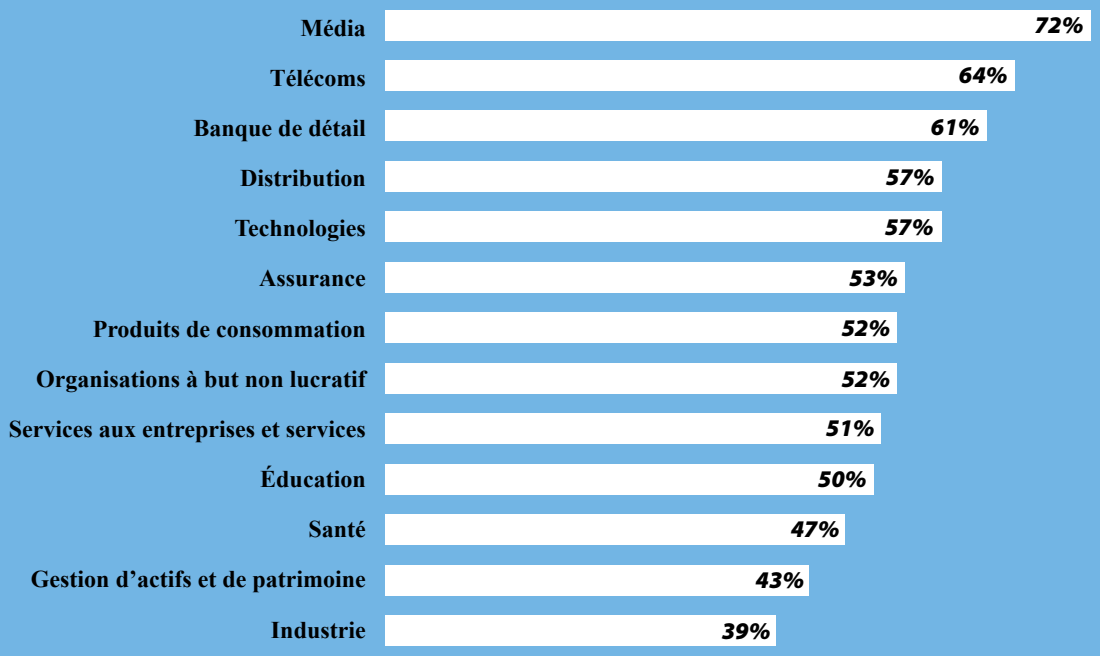
Questions clés :

- Tous les projets de transformation sont-ils gérés efficacement ?
- L'organisation a-t-elle un processus pour identifier les menaces et les opportunités technologiques émergentes ? Est-il robuste ?
- Les projets de R&D et d'innovation de l'organisation sont-ils tous cartographiés ?
- Y a-t-il un processus de management des risques en place pour évaluer la validité de ces projets, incluant l'audit interne, dans les phases initiales et de façon continue ?
- L'organisation réfléchit-elle au « pourquoi ? » ainsi qu'au « comment ? » quand il s'agit d'innovation ?
- L'entreprise évalue-t-elle l'innovation à court, moyen et long terme ?
- L'organisation a-t-elle les compétences nécessaires pour assurer le succès de ses innovations ?
- Le ROI des dépenses de R&D est-il correctement mesuré et contribue-t-il aux décisions d'investissement ?
- L'organisation a-t-elle la réactivité et la souplesse nécessaires pour accroître ou diminuer l'innovation si nécessaire ?
- Le Conseil ou la direction générale ont-ils des attentes pour que l'audit interne donne une assurance concernant la robustesse de la gestion des projets au sein de l'organisation ?

Les secteurs les plus bouleversés par le numérique

Avis des cadres dirigeants sur les secteurs qui affronteront des bouleversements modérés ou massifs liés au numérique dans les 12 prochains mois

Source : Russell Reynolds Associates



« L'enjeu **du numérique et de l'innovation** est très important dans la distribution et pour de nombreux autres secteurs. La **menace stratégique** des technologies de rupture s'accompagne de la perte potentielle d'un avantage compétitif. Il s'agit par exemple, d'un projet de **réalité virtuelle** pour améliorer l'expérience client ou de l'utilisation de **drones** pour parcourir le dernier kilomètre pour la livraison du produit. Cela va très vite et s'accompagne de risques inhérents ».

Responsable de l'audit interne, groupe international néerlandais de distribution de produits alimentaires et électroniques

INCERTITUDE POLITIQUE : BREXIT ET AUTRES INCONNUES

Les résultats du référendum sur le Brexit et de l'élection présidentielle aux États-Unis ont de profondes répercussions sur le panorama des risques. À ce jour, les négociations pour le Brexit ont à peine commencé et les réformes des politiques commerciales audacieuses et protectionnistes qui étaient au cœur de la campagne de Donald Trump ne se sont toujours pas matérialisées. Mais ces deux événements pourraient entraîner des changements significatifs – or pas de changement sans risque.

Intrinsèquement, le Brexit et la stabilité de l'Union européenne ne sont pas à proprement parler des risques. Mais le Brexit aura des répercussions sur des domaines clés comme l'immigration et les échanges commerciaux, qui pourraient tous les deux avoir une incidence significative en termes d'emploi et de chaînes d'approvisionnement. Les taux de change ont d'ores et déjà connu une certaine volatilité, augmentant les risques de change pour les organisations qui ne bénéficient pas de la couverture automatique liée à l'étendue et à la diversité de leur implantation géographique.

Dans un monde qui sort à peine d'un régime de rigueur monétaire dans lequel la croissance a été relativement faible et soutenue par la politique des banques centrales, toute évolution politique brutale autour des échanges commerciaux et de la libre circulation des travailleurs pourrait provoquer une érosion de la confiance et fragiliser les économies.

Le mot clé est « pourrait ». Il est difficile pour les organisations de se préparer à l'impact des négociations politiques et législatives quand leur résultat est inconnu ; par exemple, seules 29 % des organisations au Royaume-Uni ont fait des plans pour la sortie de l'Union européenne, ce qui est probablement dû au manque d'éléments significatifs sur lesquels baser un plan. Cependant, il est plus inquiétant que plus de la moitié (57 %) des organisations n'ont même pas discuté des risques auxquels le Brexit les expose[11].

Le futur de l'Union européenne

Début 2017, un certain nombre d'élections clés semblaient pencher en faveur de partis politiques de l'extrême-droite, soulevant des inquiétudes pour le futur de l'Union européenne. Les partis populistes avaient connu une montée en puissance importante en faisant campagne sur l'afflux de migrants, et avaient exploité le sentiment nationaliste soucieux de retrouver leur souveraineté par rapport à l'Union européenne dans la foulée du Brexit.

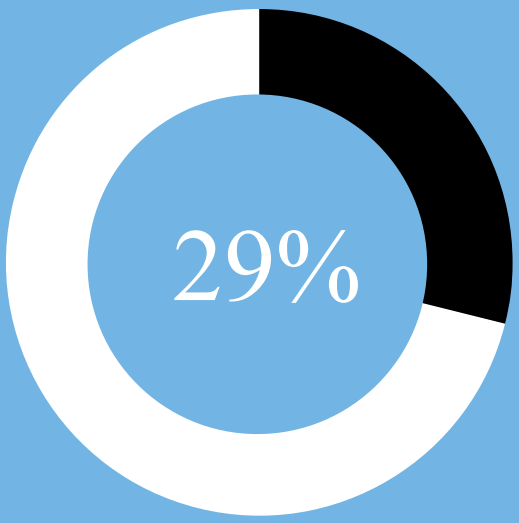
« **Le Brexit** aura une place prépondérante dans le plan d'audit de l'année prochaine. Il **est difficile de savoir quel en sera l'impact.** Actuellement nous travaillons sur la résilience – c'est-à-dire, indépendamment de ce qui se passera, quelle est notre agilité et notre rapidité à **réagir, alors que la situation se dessine,** et à définir un scénario sur le futur modèle ? On ne sait pas ce qui va se passer, mais **le niveau de résilience des organisations** face à ces changements potentiels va devenir une thématique de plus en plus importante, et je pense que cela **changera tout au long de l'année.** Donc nous prévoyons de consacrer du temps pour des travaux liés au Brexit sans savoir nécessairement à ce stade ce que nous allons faire ».

Responsable de l'audit interne, Groupe d'ingénierie et de production du FTSE 100

« Il s'agit de réfléchir à **l'impact** du **Brexit** pour notre organisation. Dès que nous saurons quels seront certains de ces effets nous devrons préparer des plans et **réagir en conséquence.** Actuellement, c'est surtout une question de surveillance, en essayant de nous projeter à trois ans. Nous n'avons pas effectué une mission formelle d'**audit du Brexit.** Néanmoins, au fil des travaux nous posons cette question : « Est-ce la bonne décision ? Le Brexit aura-t-il un impact ? ». Nous jouons plutôt un **rôle de conseil** ».

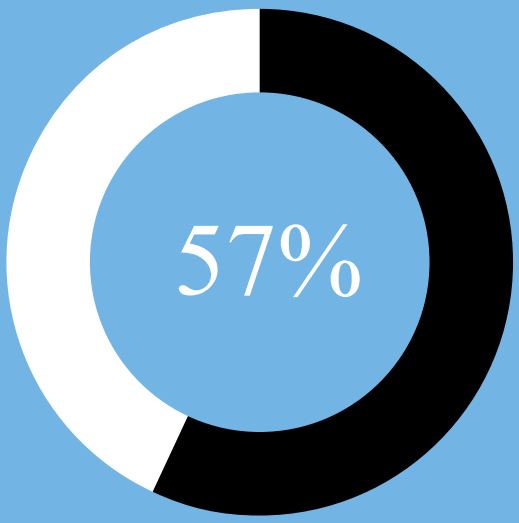
Responsable de l'audit interne, groupe de distribution au FTSE 100 Royaume-Uni

Un faible niveau de préparation au Brexit



Seules 29 % des organisations ont fait des plans relatifs à la sortie de l'Union européenne

Source : ICAEW



57 % des organisations n'ont même pas discuté des risques que le Brexit leur fait courir

Source : ICAEW

« **Le Brexit demande de la souplesse.** Le contexte n'est pas encore stabilisé, la planification se fait sans allouer du temps à des travaux précis. Dans d'autres domaines, il serait beaucoup plus facile de réfléchir à des **scénarios possibles** et d'examiner la pertinence de l'approche de l'organisation. Pour le moment, nous demandons : « **Y a-t-il une réflexion au niveau de votre service sur les conséquences que pourraient avoir le Brexit sur vos activités ? » ».**

Administrateur, agence gouvernementale du Royaume-Uni

Emmanuel Macron a battu la candidate de l'extrême droite Marine Le Pen, au deuxième tour de l'élection présidentielle française de 2017. Ces résultats ont été suivis par la défaite du populiste anti-européen Geert Wilders face au premier ministre Mark Rutte lors des élections aux Pays-Bas. Ces deux résultats peuvent être interprétés comme une victoire des courants politiques classiques et un rejet du populisme porté par l'extrême droite.

En Allemagne et en Italie, qui ont également connu une poussée de l'extrême droite, des élections sont respectivement prévues en septembre 2017 et d'ici fin 2018. Jusqu'à présent, il n'y a pas de partis eurosceptiques en Allemagne et les sondages montrent que seuls 24 % des Allemands voteraient une sortie de l'Union européenne[12].

La question de l'immigration s'invitera dans ces élections. Malgré une diminution par rapport à la crise de 2015, la pression migratoire se fait particulièrement sentir en Italie. Ces derniers mois, l'opinion semble attirée vers l'extrême droite et par des partis qui pourraient favoriser la réintroduction d'une monnaie nationale voire une sortie totale de l'Union européenne.

Une fois de plus, « pourrait » est le mot clé et l'incertitude est ce qui définit ces risques politiques. En tout cas, l'avenir du projet européen n'est pas assuré. Dans toute l'Union, les organisations devraient prendre en compte la possibilité de changements significatifs et déterminer si elles sont préparées à réagir, et à résister à ces évolutions politiques.

Jusqu'à récemment, la plupart des organisations restaient largement indifférentes à la couleur politique des gouvernements. En effet, que ceux-ci soient de gauche ou de droite, les politiques étaient plutôt libéraux et favorables au développement économique. Cependant, la polarisation s'est accentuée et la montée de partis nationalistes avec des programmes économiques anti-immigration et protectionnistes menace le commerce extérieur. Les mesures discriminatoires contre les travailleurs et les biens étrangers susciteront des risques significatifs pour les organisations.

Du point de vue de l'audit interne

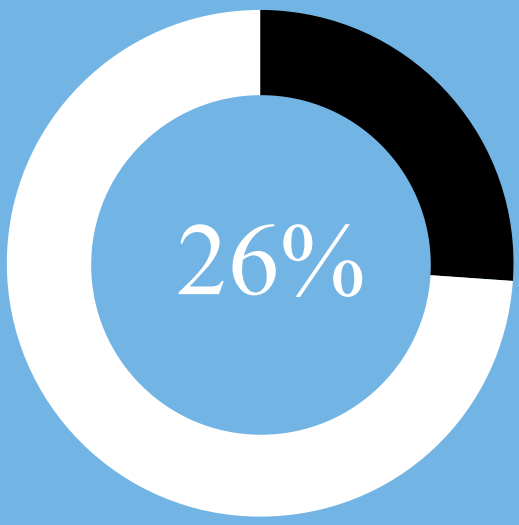
Étant donné l'imprévisibilité du Brexit, de l'avenir de l'Union européenne, de l'orientation de l'administration Trump et d'autres inconnues politiques et géopolitiques, il est difficile pour l'audit interne et les autres prestataires d'assurance de faire des recommandations spécifiques et détaillées à leur organisation.

À ce stade, la préoccupation majeure est la résilience de l'organisation. L'audit interne devra donner l'assurance que les organisations sont suffisamment souples et réactives pour adapter rapidement leurs opérations à un paysage politique incertain, changeant. La fonction d'audit interne devrait aussi examiner si l'organisation a un processus en place pour identifier les changements politiques potentiels, si la direction générale réfléchit à ces évolutions et à leur impact spécifique sur l'organisation. Un rôle de conseil peut être tenu dans les groupes de travail multidisciplinaires sur le Brexit et les risques politiques. La plupart considèrent que des missions d'audit formelles ne seront pas nécessaires ni souhaitées avant que les politiques ne se précisent. Une fois que les futures politiques sur l'immigration, le commerce et les autres sujets seront clarifiées, la fonction d'audit interne devrait s'assurer que l'organisation réagit et a réagi efficacement à ces changements.

Questions clés :

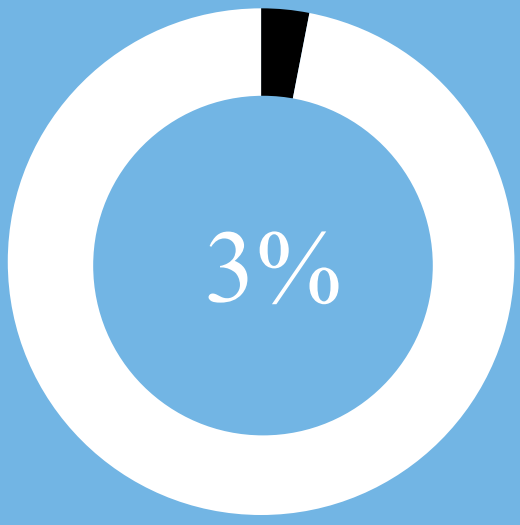
- L'organisation a-t-elle un processus en place pour identifier les risques politiques ?
- La direction générale a-t-elle réfléchi à ce que certains risques politiques spécifiques signifient pour l'organisation ? Cette analyse a-t-elle été déclinée au niveau des différentes unités opérationnelles ?
- Cette analyse détaillée a-t-elle été étendue aux chaînes d'approvisionnement et aux autres tiers ?
- La fonction de trésorerie gère-t-elle / couvre-t-elle efficacement le risque de change ?
- La direction générale a-t-elle réfléchi aux scénarios les plus pessimistes concernant les barrières à l'immigration, les droits de douane, les réformes fiscales et monétaires et envisagé la manière dont l'organisation pourrait y répondre efficacement ?
- L'organisation est-elle assez souple pour adapter ses opérations si nécessaire ?

Les risques politiques, une priorité pour les assureurs



Cette année, les risques politiques étaient les principaux risques macroéconomiques pour 26 % des assureurs

Source : Goldman Sachs Asset Management



En 2016, seulement 3 % des personnes interrogées les identifiaient comme les risques principaux

Source : Goldman Sachs Asset Management

« Des situations comme l'élection de **Donald Trump, le Brexit** et **les élections** dans de nombreux pays, représentent potentiellement un **énorme changement** dans la manière dont les organisations doivent être gérées. **Les organisations** ont besoin d'apprendre comment être **suffisamment souples** pour s'adapter.

Un plan stratégique sur trois ans peut changer en quelques mois ou même quelques semaines, donc un **plan d'urgence** est nécessaire pour être capable d'ajuster **la planification stratégique** parce que, de plus en plus, l'incertitude va être le scénario normal dans lequel **les organisations exercent leurs activités** ».

Responsable de l'audit interne,
groupe bancaire multinational espagnol

RISQUES LIES AUX FOURNISSEURS ET MAÎTRISE DE LA RELATION AVEC LES TIERS

Les risques liés aux tiers sont revenus au premier plan. En partie parce que les organisations cherchent à faire des économies grâce à l'externalisation et font de plus en plus migrer leurs opérations vers des services *cloud*. Le fameux « faire ou faire faire » concerne désormais des composants de base que les industriels préfèrent assembler au lieu de les fabriquer. Ainsi, les processus et les actifs qui étaient auparavant hébergés en interne sont hors de l'organisation, cependant ils doivent être efficacement gérés et sécurisés.

Les risques sous-jacents sont liés à la résilience et à la réputation de l'organisation (voir l'encadré à droite). L'organisation doit comprendre son degré d'exposition à une interruption potentielle causée par un fournisseur tiers qui subit une cyber-attaque, perd sa licence d'exploitation, devient insolvable ou tout simplement n'arrive pas à satisfaire une demande croissante ; les tiers devraient être répertoriés et une évaluation des risques menée pour estimer la probabilité et la sévérité des risques liés à un tiers ou un fournisseur donné.

Il faut avoir une vision claire de la manière dont l'organisation répondrait à une telle situation et des plans d'urgence pour maintenir la continuité d'activité. Pour ce faire, l'évaluation de la résilience des activités des tiers eux-mêmes est nécessaire en examinant et en s'interrogeant sur leur gouvernance et leurs dispositifs de contrôle.

C'est là que des procédures solides de diligence raisonnable sont essentielles. Quand l'organisation sélectionne un nouveau fournisseur, l'analyse devrait aller au-delà des produits et des services que le fournisseur offre et de sa capacité à les livrer. Il convient également de prendre en compte la priorité que le tiers lui-même donne à la résilience de ses activités et à la gestion efficace de ses propres risques notamment en matière de corruption, de cybersécurité et de protection des données.

La question des droits de l'homme

Concernant les risques liés aux tiers, il ne s'agit pas seulement de s'assurer de la résilience des activités et de protéger la réputation de l'organisation. Il y a aussi un certain nombre d'évolutions législatives concernant les droits de l'homme qui ont porté ces risques au premier rang des priorités. Par exemple, la loi britannique contre l'esclavage moderne incite les organisations à s'assurer qu'elles peuvent remplir les déclarations obligatoires sur la transparence mettant en évidence leurs efforts pour éradiquer les violations des droits de l'homme, en interne et dans leurs chaînes d'approvisionnement. D'autres pays ont adopté leur propre législation qui a pour objectif d'arrêter le travail forcé dans les chaînes d'approvisionnement. Dans un environnement mondialisé, ceci soulève une question importante : jusqu'à quels niveaux des chaînes d'approvisionnement les missions d'assurance doivent-elles aller ? La réponse dépendra de l'appétence pour le risque de l'organisation.

Risques de réputation par tiers interposé

On a tendance à supposer qu'externaliser signifie externaliser les risques, mais les crises qui affectent les tiers remontent habituellement jusqu'aux organisations clientes, qui ont généralement une plus grande notoriété et présentent plus d'intérêt médiatique. En particulier, quand la crise en question implique la perte de données client, lorsque le tiers est indirectement financé par l'argent des contribuables ou que le service est orienté client.

Par exemple, la violation de données de TalkTalk qui a coûté à l'entreprise britannique de télécommunication 100 000 clients était le résultat d'une cyber-attaque qui a eu lieu par l'intermédiaire d'un tiers qui avait accès au réseau de la société.

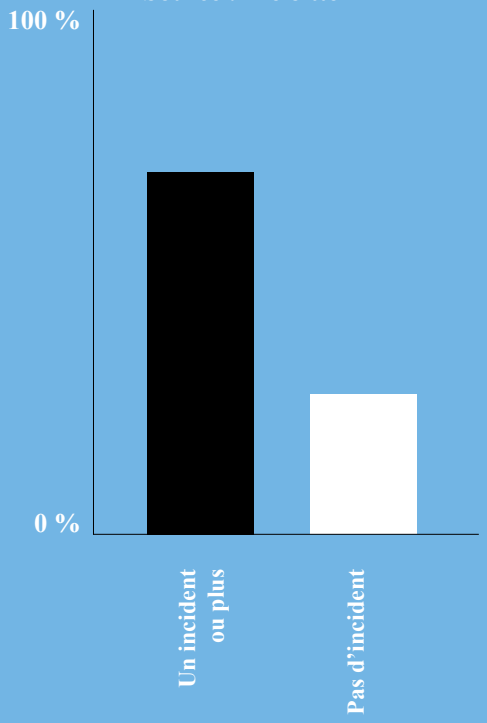
Par ailleurs, les suicides dans les usines de Foxconn en Chine liés aux bas salaires et aux mauvaises conditions de travail déclenchèrent une tempête dans les médias contre Apple parce que ces usines contribuaient à la fabrication du très populaire iPhone.

De la même manière, des distributeurs comme Primark et Matalan se sont retrouvés entraînés dans l'effondrement tragique de Rana Plaza, une usine bangladaise qui faisait partie de leur chaîne d'approvisionnement, dans lequel 1 400 employés ont perdu la vie.

Incidents liés à des tiers

74,1 % des sociétés multinationales ont fait face à au moins un incident lié à un tiers pendant les trois dernières années

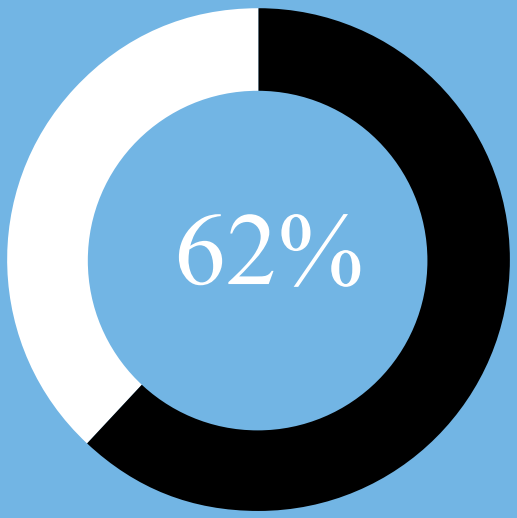
Source : Deloitte



Diligence raisonnable des fournisseurs

Les sociétés multinationales exercent une diligence raisonnable pour seulement 62 % de leurs fournisseurs, distributeurs et tiers avec qui ils sont en relation

Source : Thomson Reuters



« **Obtenir une assurance sur l'environnement de contrôle** des tiers devient plus pertinent pour notre organisation. Nous **externalisons une partie de plus en plus** importante de nos activités, surtout celles qui concernent les systèmes d'information et le *cloud*. Tout le monde **se focalise** sur l'**optimisation des activités,** mais personne ne s'intéresse aux implications en termes de **risques,** ni par conséquent, de l'assurance qu'ils devraient obtenir des tiers. La compréhension de ces risques et de leur **niveau d'assurance** doit être améliorée ».

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

En France, la nouvelle loi sur le devoir de vigilance, exige que l'organisation cliente évalue et surveille l'engagement du prestataire pour la prévention des risques concernant l'environnement, les droits de l'homme et la corruption. En 2017, le parlement néerlandais a proposé une loi qui, si elle est promulguée, nécessitera des investigations sur le travail des enfants dans les opérations et les chaînes d'approvisionnement des entreprises. Cette loi s'appliquerait non seulement aux entreprises domiciliées aux Pays-Bas, mais également aux sociétés vendant des produits aux consommateurs néerlandais, y compris par le commerce en ligne. Cependant, les petites entreprises seraient exemptées.

De même, l'Italie s'est engagée l'année dernière dans un Plan national d'action à cinq ans sur les droits de l'homme et les entreprises, qui met l'accent sur l'intégrité éthique des chaînes d'approvisionnement, conformément aux Principes directeurs de l'ONU relatifs aux entreprises et aux droits de l'homme.

Les décisions politiques placent de plus en plus les droits de l'homme au cœur de la réglementation des affaires et cette tendance devrait s'accentuer au fur et à mesure que des pays adoptent les meilleures pratiques. Les processus robustes de diligence raisonnable deviennent donc essentiels et devraient associer les questions relatives aux droits de l'homme avec la revue de la résilience de l'organisation et les autres risques liés aux prestataires essentiels.

« Les **transformations et la pérennité** de la chaîne d'approvisionnement sont **importantes** et nous conduisent à réaliser des missions d'audit des risques liés aux tiers et à la continuité d'activité de notre propre société. Il ne s'agit pas seulement **des interruptions de l'activité production,** mais également **des enjeux liés à la qualité** et au coût de livraison. L'audit interne doit se demander combien de couches l'organisation doit **éplucher** pour aller dans les **profondeurs de la chaîne d'approvisionnement.** Qu'est-ce qui est nécessaire ? Quels risques l'organisation est-elle prête à prendre ? Ceci a-t-il bien été énoncé ? Des mesures d'atténuation sont-elles en place ? Est-ce que chacun comprend les **risques qu'il prend** ? »

Responsable de l'audit interne, Groupe d'ingénierie et de production au Royaume-Uni

Du point de vue de l'audit interne

L'audit interne a un rôle essentiel à jouer pour donner une assurance sur les risques liés à la chaîne d'approvisionnement. Au niveau élémentaire, l'organisation doit avoir l'assurance que ses fournisseurs peuvent livrer le produit ou le service souhaité, y compris augmenter ou diminuer la production ou le service à la demande. Mais l'importance croissante accordée aux droits de l'homme, à la cybersécurité, à une gouvernance forte contre la corruption et à des normes environnementales exigeantes – et les répercussions d'incidents qui se sont produits chez des tiers sur la réputation de l'organisation – signifient que la diligence raisonnable des fournisseurs et des prestataires n'a jamais été aussi importante.

L'audit interne peut apporter de la valeur ajoutée en examinant la gouvernance des approvisionnements et la gestion des contrats, en vérifiant que les contrats comprennent formellement une clause d'audit et que les fournisseurs ont de solides procédures d'alerte en place. La coordination avec la fonction d'approvisionnement permet de s'assurer que les processus de diligence raisonnable sont exhaustifs et répondent aux besoins d'atténuation des risques de l'organisation. Un enjeu majeur est de décider jusqu'où les missions d'audit et les activités d'assurance doivent aller dans la chaîne d'approvisionnement. Elles dépendront du niveau de risques auquel l'organisation est prête à s'exposer et des ressources disponibles pour ces activités d'assurance.

Questions clés :

- Une évaluation exhaustive des risques liés aux tiers a-t-elle été menée pour cartographier les prestations externes (par exemple l'approvisionnement, la logistique, la distribution, la fabrication, l'hébergement dans le *cloud*…) et l'exposition aux risques de l'organisation ?
- L'organisation a-t-elle l'assurance que ses fournisseurs pourront faire face à toute hausse de la demande ?
- Les approvisionnements sont-ils soutenus par des processus robustes de diligence raisonnable pour évaluer la gouvernance et le profil de risque des fournisseurs externes ?
- Quel est le niveau d'assurance quant à l'efficacité de la gestion des risques par les tiers, y compris la résilience de leurs activités, la cybersécurité et la corruption ?
- Les tiers sont-ils en conformité avec la nouvelle législation relative aux droits de l'homme ?
- Y a-t-il eu une cotation du risque pour les fournisseurs et les tiers selon leur situation géographique et leur secteur, et par conséquent leur exposition aux risques concernant les droits de l'homme, la corruption et aux autres risques ?
- L'organisation a-t-elle l'assurance que le niveau de risques auquel sont exposés les tiers avec lesquels elle est en relation est en adéquation avec sa propre appétence pour le risque ?
- L'organisation a-t-elle l'assurance que le comportement des tiers n'affecte pas son risque de réputation ?
- L'organisation a-t-elle un plan d'urgence en place dans l'éventualité d'une perte d'exploitation d'un tiers ou d'un incident affectant sa réputation ?

« **Nos tiers** vont des **gestionnaires de pensions de retraite**, des prestataires pour la fonction finance à, plus récemment, la **gestion** des **données client**. Au-delà de la conformité avec le RGPD, nos **clients nous confient** leurs données personnelles et nous ne voulons pas trahir cette confiance. Ainsi, s'assurer que les tiers **gèrent nos données efficacement** et en toute sécurité est important. Le management peut parfois penser que les risques ne sont plus les leurs quand ils externalisent, mais ce n'est pas le cas.

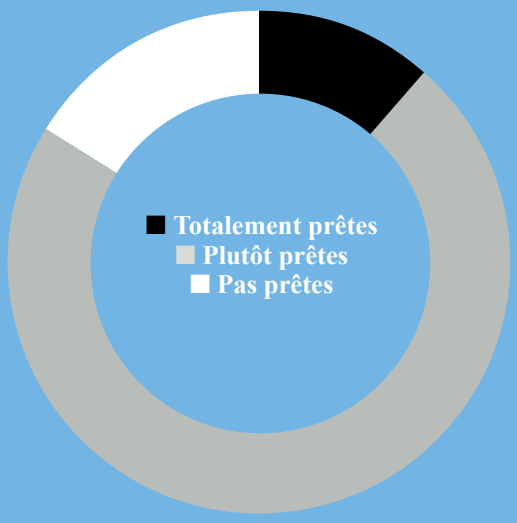
Nous devons **aider le management à comprendre les risques liés aux tiers** et à savoir si l'organisation arrive à suivre l'évolution de ses relations ».

Responsable de l'audit interne, Groupe néerlandais de distribution multinational

Incertitudes liées à des tiers

Seules 11,6 % des sociétés ont le sentiment d'être « totalement prêtes » à faire face à l'incertitude croissante dans l'environnement externe, alors que 72,3 % se sentent « plutôt prêtes » et que 16,1 % ne sont « pas prêtes » à faire face à cette incertitude

Source : Deloitte



LA PROBLEMATIQUE DE LA CULTURE

La culture de l'organisation est maintenant devenue une priorité pour les conseils. De nombreuses organisations, particulièrement dans les secteurs des établissements financiers et de l'énergie, ont perdu la confiance du public et cherchent à rétablir leur réputation. Les problématiques et les incidents qui ont porté atteinte à la réputation ont largement été le résultat direct ou indirect d'une faible culture de l'organisation.

Développer une culture robuste et l'exemplarité au plus haut niveau est essentiel pour maîtriser les risques de réputation et de conformité, ainsi que pour la création de valeur à long terme. Mais comment les organisations s'assurent-elles que l'exemplarité au plus haut niveau reflète les valeurs de l'organisation ? Comment les conseils peuvent-ils s'assurer que l'exemplarité se répercute effectivement vers l'encadrement intermédiaire et à la base ? Comment la culture est-elle évaluée, et si elle est jugée insuffisante, comment la faire évoluer ? Ces questions sont toujours à l'ordre du jour dans les organisations.

Tout d'abord, il est important de définir ce que l'on entend par culture. Dans une organisation, il s'agit des valeurs, attitudes, principes et croyances partagés qui caractérisent ses membres et la définissent. Par conséquent, une des étapes les plus importantes pour être capable d'évaluer la culture de l'organisation est de comprendre si le personnel se sent capable de signaler un comportement inadéquat ou un méfait du management sans crainte de représailles. Si les personnes au sein de l'organisation sont trop effrayées pour s'exprimer, il sera difficile de détecter les mauvaises pratiques.

Du sommet à la base

En fin de compte, une culture solide commence avec une direction forte et une communication adéquate du but et de la stratégie de l'organisation. Les collaborateurs ont besoin de se sentir estimés et d'avoir le sentiment qu'eux-mêmes et leur conduite et leur comportement font partie intégrante de la capacité de l'organisation à atteindre ses objectifs, ajustant ainsi leurs valeurs personnelles avec celles de l'organisation.

Une erreur courante est de supposer qu'en développant l'exemplarité adéquate au plus haut niveau, celle-ci ruissellera dans toute l'organisation. En réalité, ce n'est pas toujours le cas dans les multinationales où les unités opérationnelles locales ont leur culture endogène et leurs façons de travailler. Au lieu de cela, la direction générale devrait exiger du management un comportement adéquat et encourager l'exemplarité désirée au niveau de l'encadrement intermédiaire.

Dans de nombreux cas, la culture des risques d'une organisation n'est pas en adéquation avec les valeurs qu'elle professe ni avec ce qu'elle affirme être. Dans le secteur bancaire, certaines sociétés se sont présentées comme des prêteurs responsables alors que dans le même temps elles employaient des systèmes d'incitation et des objectifs commerciaux agressifs qui ont encouragé la vente abusive de produits. Une mesure clé, par conséquent, est de s'assurer que les modèles commerciaux n'encouragent pas des comportements indésirables et même des violations de la conformité (voir l'encadré, ci-dessus).

Évaluer et redéfinir la culture ne signifie pas seulement éradiquer les comportements indésirables, comme des

La coalition de la culture

En 2016, le *Financial Reporting Council*, le régulateur indépendant pour le Royaume-Uni et l'Irlande qui a la responsabilité de promouvoir une gouvernance et un reporting de grande qualité, publia un rapport sur la culture de l'organisation qui s'inspirait des recherches et travaux d'un certain nombre de partenaires, y compris l'IIA UK *(Chartered Institue of Internal Auditors).* Cette « coalition de la culture » a identifié trois enjeux importants à considérer quand il s'agit de prendre des mesures dans ce domaine.

Relier mission, stratégie et culture. Définir la mission de l'organisation est essentiel pour soutenir ses valeurs et encourager les comportements adéquats. La stratégie pour réaliser la mission de l'organisation devrait refléter ses valeurs et sa culture et ne devrait pas être conçue isolément. Les conseils devraient superviser chacun de ces aspects.

Ajuster valeurs et incitations. Le recrutement, la gestion de la performance et les récompenses devraient soutenir et encourager des comportements en adéquation avec la mission, les valeurs, la stratégie et le modèle économique de l'organisation. Un équilibre judicieux devrait être trouvé entre les incitations financières et non financières, et elles devraient être reliées à des objectifs de comportement positif.

Évaluer et mesurer. Les conseils devraient réfléchir soigneusement à la manière dont la culture est évaluée et la communication à cet égard. Un large éventail d'indicateurs potentiels est disponible. Les sociétés peuvent choisir et suivre ceux qui sont adaptés à l'organisation et aux résultats ciblés. L'évaluation objective de la culture implique d'interpréter les informations avec doigté pour obtenir des éclairages pratiques.

Pour plus d'informations, veuillez consulter : www.frc.org.uk

Modalités d'audit de la culture

L'IIA UK propose quatre modalités d'évaluation de la culture de l'organisation. Chaque organisation aura sa propre approche, que ce soit en dédiant un programme de travail spécifiquement pour ce sujet ou en adoptant une perspective plus large en incorporant les variables culturelles dans les missions d'audit existantes. Ce qui est important est de trouver une approche qui convient à votre fonction d'audit interne.

1 « Méta-audit » à partir d'observations consolidées - en utilisant des points de vue sur la culture, issus de missions d'audit spécifiques sur une période déterminée.

2 Mission d'assurance globale et exhaustive sur la culture - évaluation de la conformité et de l'efficacité par rapport aux attentes. Celles-ci doivent être de préférence définies par le Conseil.

3 Mission classique d'assurance sur un aspect donné - par exemple le fonctionnement adéquat de la structure de gouvernance par rapport au cadre prédéfini, la tenue des réunions avec les participants appropriés, la formalisation de la prise de décision, la réflexion autour des risques, la discussion des alternatives, la gestion de la pensée de groupe à travers notamment une politique adéquate de diversité.

4 Mission de conseil donnant des points de vue sur un aspect spécifique - par exemple à propos d'un projet, d'une évolution des méthodes de travail en collaborant avec la DRH pour identifier les risques et les prochaines étapes après une enquête auprès des collaborateurs.

Pour plus d'informations, veuillez consulter www.iia.org.uk/culture

« **La culture** figure assurément parmi les **priorités** du management. **38 % des collaborateurs** ont moins d'un an d'ancienneté. Dans le **secteur de la technologie,** ce chiffre est plus proche de **50 %.** Je ne sais pas combien de **nationalités** travaillent ici aujourd'hui, nous **avons cessé de compter.** Donc comment maintient-on la culture **vivante ?** Comment crée-t-on un **environnement inclusif** dans lequel les gens se sentent en sécurité pour **s'exprimer ?** »

Responsable de l'audit interne, prestataire de services informatiques multinational néerlandais

« Les banques doivent prendre des mesures proactives pour **éviter tout type de pratiques commerciales inappropriées.** Cela renvoie sans doute aux risques liés à la culture. L'organisation doit s'assurer que **ses collaborateurs connaissent les comportements** à proscrire quelles que soient les circonstances, et s'assurer que des incitations financières n'encouragent pas de comportements inappropriés. **Le changement culturel doit venir du sommet** de l'organisation. Le management doit donner l'exemple et des instructions claires et, comme tout changement, cela **prend du temps.** D'ici-là, l'audit interne doit évaluer les systèmes de contrôle pour éviter ce qui est arrivé à d'autres banques ».

Responsable de l'audit interne, groupe bancaire multinational espagnol

pratiques d'incitation qui font passer les profits devant les principes. Comme cela a déjà été mentionné dans ce rapport, les organisations subissent d'énormes transformations, particulièrement sur le front numérique. Sans un changement culturel, l'organisation s'accrochera à des comportements et des façons de faire dépassés.

Transformer une culture en l'ajustant à la future stratégie de l'organisation requiert la création d'un environnement caractérisé par des comportements ouverts au changement. La culture de l'organisation s'est, volontairement ou non, incrustée au fil des ans voire des décennies et la changer prend du temps.

Mais avant tout, l'organisation doit déterminer clairement sa stratégie à court, moyen et long terme. Elle doit comprendre ce qu'elle veut être, pourquoi et comment y parvenir. Le rythme rapide de l'innovation signifie que de nombreuses sociétés doivent transformer leur modèle économique et réfléchir sérieusement à leurs objectifs et aux critères tangibles de succès. C'est sur cette base explicite que l'organisation peut s'efforcer de créer une culture qui soutient ces nouveaux objectifs.

Uber : le coût d'une culture insuffisante

Les sociétés à la pointe du progrès et innovantes peuvent également être victimes d'une culture insuffisante. Uber, une des entreprises de haute technologie les plus performantes de la dernière décennie, a vu son PDG et fondateur Travis Kalanick évincé en 2017 pour sa mauvaise gestion de l'organisation.

Après son départ la startup a communiqué à l'issue d'une enquête de plusieurs mois sur sa culture d'entreprise. Elle a souligné que les 14 « valeurs fondamentales » de Kalanick, qui ont été à l'origine de l'organisation et ont été intégrées dans celle-ci, devaient être revues car elles avaient « été utilisées pour justifier un comportement inadéquat ».

Par exemple « marcher sur les pieds », véhiculait l'idée que la réussite dépendait du mérite, y compris celui d'écraser des personnes sur le chemin du succès ; face aux taxis traditionnels voire avec les régulateurs, il était recommandé de « toujours jouer des coudes » ; et la « confrontation de principe ». Finalement, ces valeurs et le comportement qu'elles engendraient ont coûté son poste à Kalanick. Désormais, Uber doit s'atteler à l'énorme projet de transformation de sa culture.

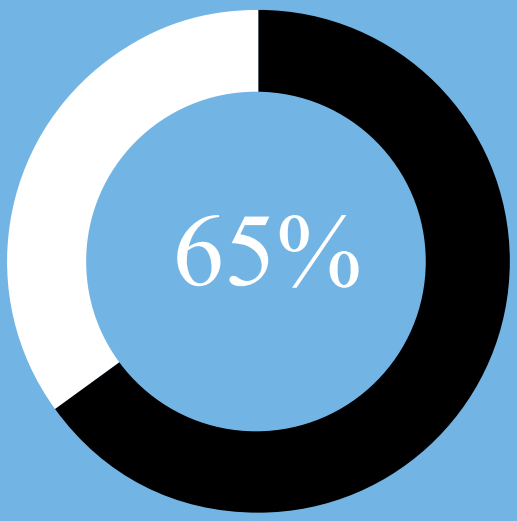
Du point de vue de l'audit interne

La problématique de la culture de l'organisation et de ses modalités d'évaluation précise occupe toujours l'esprit des responsables de l'audit interne. Certains ont mené des missions dédiées à l'audit de la culture, certains ont incorporé la variable culturelle dans chaque mission d'audit, tandis que d'autres n'ont encore rien entamé. Mais il n'en reste pas moins que les conseils souhaitent comprendre la culture de leur organisation et que l'audit interne est toujours en train d'explorer la meilleure manière d'y parvenir. L'audit interne a un rôle essentiel à jouer pour évaluer si la culture existante et les comportements reflètent la philosophie et les valeurs affichées par l'organisation, s'ils empêchent l'organisation de parvenir à la transformation qu'elle recherche et quelle est l'efficacité des mesures pour refondre la culture.

Questions clés :

- La stratégie, les objectifs et les valeurs de l'organisation sont-ils en phase avec sa culture ?
- La culture de l'organisation permet-elle d'atteindre ces objectifs à tous les niveaux de l'organisation ?
- Ce que l'organisation affirme être se reflète-t-il dans le comportement du management et des collaborateurs ?
- L'exemplarité au plus haut niveau est-elle « saine » et se répercute-t-elle effectivement dans toute l'organisation ?
- L'encadrement intermédiaire met-il l'accent sur un comportement correct qui donne une bonne image de l'organisation ?
- La DRH a-t-elle une politique d'intégration efficace pour que les nouveaux collaborateurs adoptent la culture désirée ?
- Les processus de recrutement comprennent-ils une vérification de l'adhésion des candidats aux valeurs partagées par l'organisation avant l'embauche ?
- La fonction d'audit interne a-t-elle les compétences et l'expérience nécessaires pour évaluer la culture et les indicateurs liés aux comportements ?
- Les collaborateurs se sentent-ils en confiance pour s'exprimer et signaler tout comportement ou pratique inappropriés ?
- L'organisation encourage-t-elle, directement ou indirectement, les comportements contraires à l'éthique envers ses clients ou ses propres collaborateurs ?

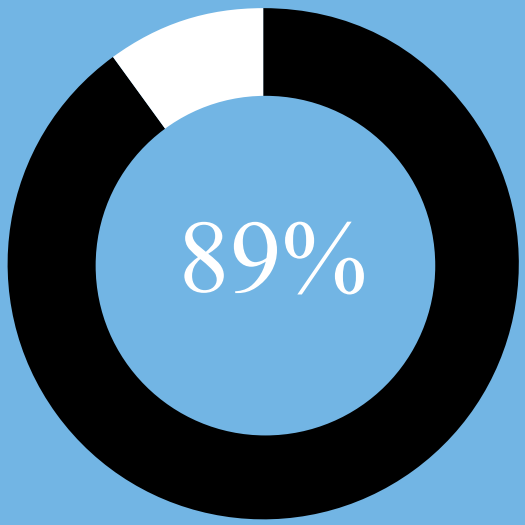
Confiance des collaborateurs



Seuls 65 % des collaborateurs disent faire confiance à l'organisation pour laquelle ils travaillent

Source : Grant Thornton

Appréciation de la confiance



89 % des collaborateurs croient que la confiance est importante pour la satisfaction professionnelle

Source : Grant Thornton

« Au **début** de chaque mission **d'audit**, nous parvenons à **cadrer** les questions liées à la **culture**. J'ai deux **collaborateurs confirmés** qui ne font rien d'autre. Jour après jour, **ils nous aident à parvenir à ces résultats.** J'ai quelqu'un dans mon équipe qui a un doctorat en **comportement au sein des organisations** et qui a travaillé pendant de nombreuses années avec les régulateurs néerlandais. Elle m'aide à concevoir notre approche. Nous la **déclinons** dans certaines entités et dans différents pays, pour donner une **conclusion étayée** au Conseil. Certaines organisations réalisent des **missions dédiées** à l'audit de la culture, mais c'est l'option que nous avons retenue et celle avec laquelle je me sens le plus à l'aise et je sais que nos pairs ont la même **approche** ».

Responsable de l'audit interne, groupe néerlandais multinational bancaire

CAPITAL HUMAIN : SE PROJETER VERS LE FUTUR

Les organisations doivent, plus que jamais, avoir une réflexion stratégique de gestion prévisionnelle des emplois, pour un certain nombre de raisons, dont l'impact démographique du départ à la retraite des *baby-boomers*.

Les organisations doivent donc anticiper suffisamment à l'avance toute pénurie liée à des rôles clés, et plus largement la manière d'attirer et de fidéliser des jeunes talents ayant les compétences nécessaires. Il convient également de créer les nouveaux postes qui assureront les succès futurs de l'organisation dans un monde de plus en plus numérique.

Aujourd'hui, la génération Y, la génération la plus jeune, est prépondérante. Cependant, il ne s'agit pas seulement d'assurer la succession des travailleurs plus âgés. Il faut savoir tenir compte du fait que cette génération a des attitudes différentes envers le travail et des attentes spécifiques en termes de carrière et de leur vie professionnelle quotidienne.

Par exemple, la génération Y apprécie la liberté de travailler avec des horaires flexibles et à distance. Comme elle est à l'aise et familiarisée avec les technologies numériques, cette génération est bien adaptée au travail à domicile. Pour la majorité des personnes (75 %) de cette tranche d'âge, l'équilibre vie professionnelle-vie personnelle motive leurs choix de carrière[13]. Les organisations doivent donc soigneusement envisager d'offrir des horaires de travail flexibles, la possibilité de travailler à domicile, des entretiens d'évaluation basés sur les résultats et les objectifs et le droit aux congés non rémunérés.

Plus que la flexibilité, les recherches montrent que plus de la moitié (51 %) de la génération Y sondent le marché pour des perspectives de carrière en-dehors de l'entreprise, comparé à 37 % de la génération X (la génération précédente) et 18 % des *baby-boomers* (la génération qui précède celle-ci)[14]. Les efforts de fidélisation des talents doivent plus que jamais être renforcés en offrant des opportunités diverses, en créant des parcours professionnels à la fois verticaux et horizontaux.

Le bien-fondé de la planification stratégique des emplois est aussi étayé par l'évolution de la nature du travail. Les responsables estiment que dans trois ans, 44 % de la population active se composera de prestataires et de postes internes temporaires. Et 79 % de ce que l'on appelle la main d'œuvre « liquide » seront affectés à des projets dynamiques plutôt qu'à des fonctions professionnelles traditionnelles, statiques[15].

Les sociétés sont soumises à une pression constante et continue pour changer leurs produits, leurs services et même leurs modèles économiques chaque fois que des nouvelles technologies ou des innovations émergent. Cela exige d'elles qu'elles soient souples concernant leurs compétences et leurs projets. Les sociétés qui ont le plus rapidement accès aux compétences nécessaires et qui réussissent mieux à faire correspondre ces compétences à leurs besoins s'adapteront et se développeront plus efficacement.

La direction générale et la DRH devraient donc réfléchir à la proportion et aux segments de la main d'œuvre permanente dans le futur ainsi qu'à l'ajustement de ces projections avec les besoins à court, moyen et long terme de l'organisation.

Automatisation

Les rapides avancées de l'intelligence artificielle (IA) et de la robotique signifient que de nombreux emplois qui étaient autrefois exclusivement occupés par des êtres humains sont, ou seront bientôt, automatisés pour la première fois. Les machines et les logiciels ne se limitent plus aux tâches de production, mais ont trouvé des applications partout, des voitures autonomes à la presse.

Par exemple, Thomson Reuters a recours à des algorithmes pour la rédaction des résultats des sociétés, libérant du temps pour que ses journalistes se concentrent sur des articles nécessitant plus d'implication. Ainsi, une couverture exhaustive des résultats boursiers est assurée plutôt que des brèves sur les bénéfices des principales capitalisations.

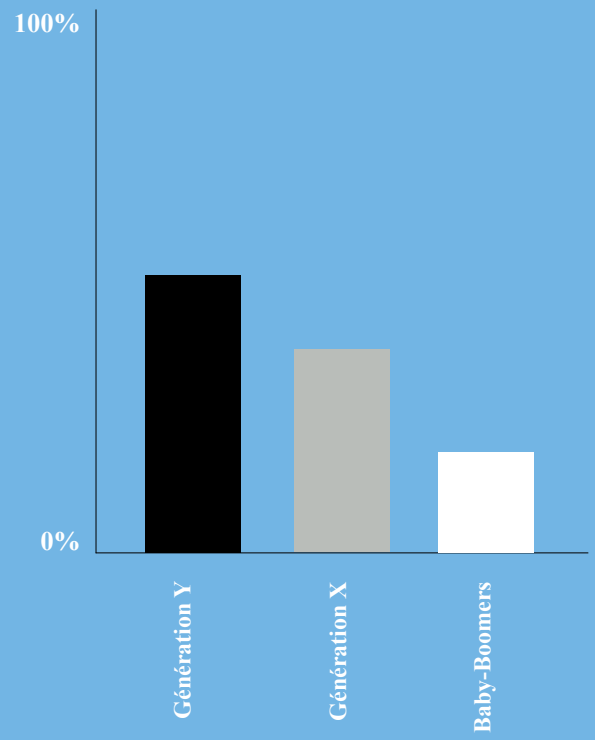
L'automatisation est la plus fréquemment citée parmi les forces perturbatrices qui auront le plus d'impact sur les organisations dans 25 ans, 51 % des sociétés la mentionnant, suivie de la réglementation (43 %), du facteur humain (38 %) et d'autres technologies qui ne sont pas encore disponibles (38 %)[16].

Les médias focalisent sur le remplacement de nombreux travailleurs. Cependant, il y aura inévitablement une interface entre les êtres humains et l'outil technologique. Ainsi, l'automatisation pourrait induire la création de millions d'emplois non prévus à ce jour. En fin de compte, les sociétés doivent réfléchir à la manière dont l'automatisation aura une incidence sur leur future main d'œuvre, ainsi que sur leurs modèles économiques.

Faire évoluer sa carrière

51 % de la génération Y cherchent des perspectives de carrière à l'extérieur, par rapport à 37 % de la génération X et 18 % des *baby-boomers*

Source : PwC



Transformer les emplois

Seules 13 % des sociétés au Royaume-Uni disent qu'elles sont prêtes à répondre aux bouleversements liés à la main d'œuvre et à créer « une organisation du futur »

Source : Deloitte

Pourtant 88 % de ces entreprises considèrent que créer l'organisation du futur est devenu une priorité

Source : Deloitte

« Les ressources humaines sont un **sujet extrêmement important** pour nous à cause de notre taille et de la pression qui s'exerce sur la fonction publique depuis un certain nombre d'années concernant les effectifs de l'administration centrale. L'efficience attendue de notre part ne concerne pas seulement les ressources financières mais également les emplois. Donc il y a énormément de travaux d'audit interne autour de la planification des emplois. Que faire si **la pyramide des âges de l'organisation** indique une main d'œuvre particulièrement vieillissante ? C'est **l'un de nos points d'attention prioritaires** pour les prochaines années ».

Administrateur, agence gouvernementale du Royaume-Uni

« Un enjeu identifié par l'organisation il y a quelque temps et **que nous contribuons à gérer** concerne les questions de ressources humaines, de fidélisation, de diversité, **d'équilibre vie professionnelle-vie personnelle** ... Le comité d'audit souhaite avoir l'assurance que l'organisation fait ce qu'elle dit qu'elle fait. **Les plus jeunes** s'attendent à pouvoir travailler différemment, avec plus de **flexibilité**. Tout cela a des répercussions sur la cybersécurité – si vous avez des collaborateurs qui travaillent à domicile alors vous avez plus de périphériques mobiles connectés à votre réseau ; les collaborateurs veulent également pouvoir se **connecter avec leurs propres appareils**. Des initiatives sont en cours dans certains pays. Elles ne posent pas en soi de problèmes, mais ces démarches doivent être **maîtrisées** et les **risques** y afférant doivent être **compris** ».

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

Le déficit de compétences se creuse

Les organisations qui transitionnent de la vieille économie analogique pour devenir des acteurs numériques prêts à saisir les opportunités offertes par les technologies émergentes, ont des besoins accrus de compétences en système d'information, en gestion des données et dans les autres domaines liés aux technologies. Les déficits de compétences doivent être comblés et les emplois doivent être transformés pour être capables d'entraîner effectivement l'organisation dans une nouvelle direction stratégique.

En Europe, le déficit de compétences s'est creusé de 14 % durant les cinq dernières années et plus particulièrement dans le domaine numérique[17]. Cela a poussé la Commission européenne à publier en décembre 2016 le Manifeste pour les compétences numériques et à lancer la coalition pour les compétences et l'emploi numérique, qui regroupe les États membres de l'Union européenne, les entreprises, les partenaires sociaux, les organisations à but non lucratif et les établissements de formation pour prendre des mesures et s'attaquer au déficit de compétences numériques en Europe.

Dans cette optique, les organisations doivent accorder une attention particulière à leurs futurs besoins en compétences et, quand cela est nécessaire, mettre en place des programmes pour attirer les personnes de talent qui ont les compétences désirées, former les collaborateurs existants et, le cas échéant avoir recours à des prestataires externes.

Du point de vue de l'audit interne

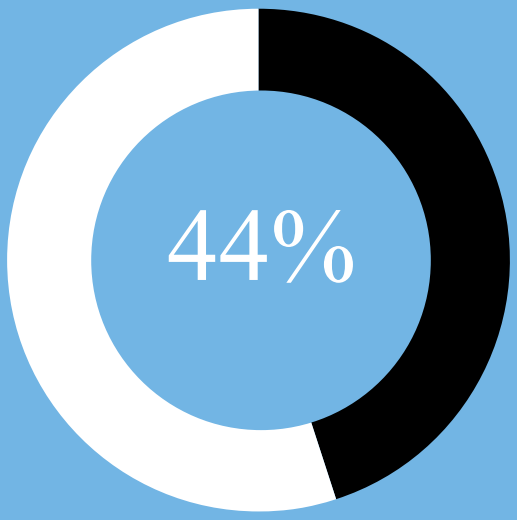
Le succès de toute organisation dépend des personnes qui y travaillent. L'incapacité à embaucher et à fidéliser les talents adéquats est donc un risque opérationnel important. À cet effet, l'audit interne doit être capable d'évaluer si les risques RH sont efficacement gérés et de donner l'assurance que la planification stratégique des emplois est conforme à sa vision stratégique. Dans quelle position l'organisation veut-elle être dans les cinq prochaines années ? Ses politiques de recrutement et de maintien dans l'entreprise supportent-elles cette orientation ?

Les compétences en système d'information, les compétences technologiques et numériques vont être très demandées dans un avenir prévisible, donc l'audit interne devrait évaluer si l'organisation fait des efforts pour réduire tout déficit actuel ou futur de compétences dans ce domaine. Les conseils souhaitent également une assurance quant à l'intégration efficace de la génération Y de sorte que ces nouveaux talents soient attirés vers l'organisation tout en répondant aux besoins des générations précédentes.

Questions clés :

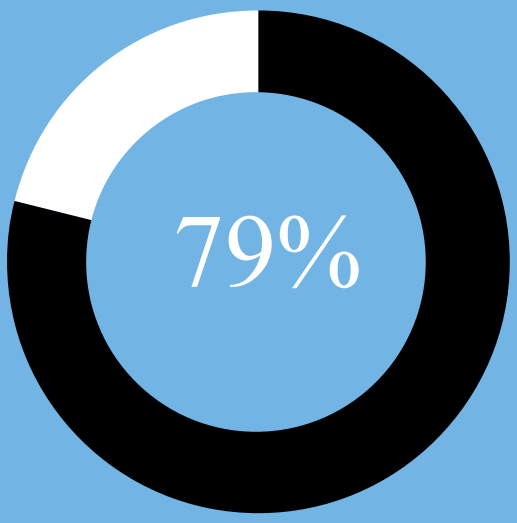
- Dans quelle mesure l'organisation a-t-elle évalué ses déficits actuels et futurs de compétences ?
- L'organisation est-elle dotée des compétences adéquates en système d'information et dans le domaine du numérique ?
- La stratégie en matière de ressources humaines est-elle alignée avec la stratégie globale de l'organisation ? Les politiques de recrutement et de maintien dans l'organisation soutiennent-elles ses objectifs futurs ?
- L'organisation a-t-elle réfléchi à la structure démographique des emplois et à la manière dont le départ à la retraite des baby-boomers va affecter ses opérations ?
- Les politiques d'attractivité de talents plus jeunes grâce à des dispositifs de flexibilité de l'organisation du travail et des opportunités professionnelles diverses sont-elles suffisantes ?
- L'organisation est-elle dans un secteur qui sera vraisemblablement rattrapé par l'automatisation, et comment cela affectera-t-il les emplois ?
- L'organisation a-t-elle envisagé l'impact de la notion de main d'œuvre « liquide » dans son contexte et la capacité de la DRH à gérer la recherche de talents spécifiques pour répondre à l'évolution des besoins opérationnels ?

La main d'œuvre liquide



Les dirigeants estiment que dans trois ans la population active sera composée de 44 % de prestataires et de postes internes temporaires - la main d'œuvre « liquide »

Source : Accenture



79 % de cette dite main d'œuvre dite «liquide» seront affectés à des projets dynamiques plutôt qu'à des fonctions traditionnelles, statiques

Source : Accenture

« **La gestion des personnes** est un enjeu important dans le contexte d'un **travail collaboratif,** d'une gestion des projets, d'une **mise en réseau** et **d'une autonomie de gestion** plus importants **par opposition** à un contrôle hiérarchique étroit. Les rôles et les responsabilités doivent évoluer, particulièrement ceux des personnes en charge des RH et du management, mais les résultats de ces **évolutions doivent faire l'objet d'une critique constructive.** L'audit interne doit prendre en compte les problématiques transgénérationnelles, le stress au travail, ainsi que la mobilité générale et professionnelle qui devront peut-être être plus transitoires pour faire face aux besoins en compétences en phase avec le rythme du **changement dans l'organisation** ».

Responsable de l'audit interne, groupe industriel français

TRANSFORMER LA FONCTION D'AUDIT INTERNE

Les attentes envers l'audit interne n'ont jamais été aussi grandes et comme les profils de risque des organisations évoluent avec le temps, il en va de même pour le niveau d'assurance attendu. Pourtant, une bonne partie des travaux de l'audit interne continue à être centré sur l'évaluation des risques opérationnels et sur les dispositifs de contrôle interne mis en place pour atténuer ces risques.

Les organisations s'intéressent de plus en plus aux menaces externes comme les cyber-attaques, l'impact du Brexit et d'autres évènements politiques, et les risques stratégiques liés à l'évolution rapide des technologies et aux modèles économiques en rupture. L'audit interne doit également avoir cette ouverture vers l'écosystème.

Certaines organisations bénéficieront d'une augmentation du budget de l'audit interne, mais pour beaucoup, l'accroissement des attentes signifie en faire plus à ressources constantes. Par conséquent, la définition des travaux d'audit prioritaires doit être efficace, les plans d'audit fondés sur une approche par les risques devront plus que jamais répondre aux besoins de l'organisation, les prestations des missions d'audit et le niveau d'assurance fournie devront être améliorés par des méthodes plus efficaces, des embauches ou de la co-traitance avec des experts, l'analyse de données et d'autres technologies.

Les responsables de l'audit interne devront identifier la manière dont leur fonction répond aux besoins de maîtrise des risques de leur organisation et trouver une solution aux déficits de compétences grâce au recrutement, à la co-traitance ou à l'externalisation. Pour optimiser le temps et les ressources, ils devront également envisager de faire évoluer les méthodes et référentiels d'audit existants.

Selon l'organisation, les domaines suivants retiendront peut-être l'attention pour s'assurer que la fonction d'audit interne atteint son plein potentiel.

L'audit « agile »

L'approche « agile » est largement utilisée dans la gestion de projets et le développement de logiciels - et commence maintenant à trouver des applications dans l'audit interne. Elle est centrée sur l'amélioration constante, la flexibilité du champ d'application, les points de vue des membres de l'équipe et la réalisation de livrables-clés. En audit interne, une telle démarche implique une coordination étroite entre les missions d'audit et entre les membres de la fonction, la collaboration avec les audités (tout en gardant son indépendance), et la prise en compte de l'évolution des besoins pendant les missions d'audit et au fil du plan d'audit. Les missions d'audit se déroulent par « vagues » et des « mêlées » permettent aux membres de l'équipe de partager régulièrement les progrès et les connaissances.

Les bénéfices de l'analyse des données pour l'audit interne

Le potentiel de l'analyse de données n'est limité que par la disponibilité des données à analyser et la capacité des auditeurs à être créatifs sur ses modalités d'application. Un rapport récent de l'IIA UK a identifié les bénéfices suivants :

- l'efficience. Par exemple, les scripts peuvent être réutilisés pour des missions d'audit régulières, ce qui se traduit par une utilisation efficiente de l'analyse de données par rapport aux analyses non automatisées ;
- l'efficacité par des contrôles sur la population entière plutôt que sur des échantillonnages aléatoires ou fondés sur le jugement professionnel ;
- un niveau d'assurance accru ;
- l'accent mis sur les risques stratégiques par rapport à des tâches plus routinières qui peuvent être automatisées dans une plus large mesure ;
- un périmètre d'audit élargi ;
- des économies importantes, de temps et de coûts, sur le long terme.

Vous pouvez trouver le rapport complet à : www.iia.org.uk/dataanalytics

Valeur ajoutée

L'audit interne ne se résume pas à un strict contrôle de conformité. Il s'agit d'apporter de la valeur ajoutée chaque fois que cela est nécessaire. Étant donné leur expertise en matière de gouvernance, de management des risques et de contrôle interne, les directeurs de l'audit interne ont parfois des responsabilités supplémentaires, qui peuvent inclure une aide à la décision fondée sur leur point de vue concernant le management des risques de l'organisation et les domaines où le niveau d'assurance est inadéquat ou insuffisant.

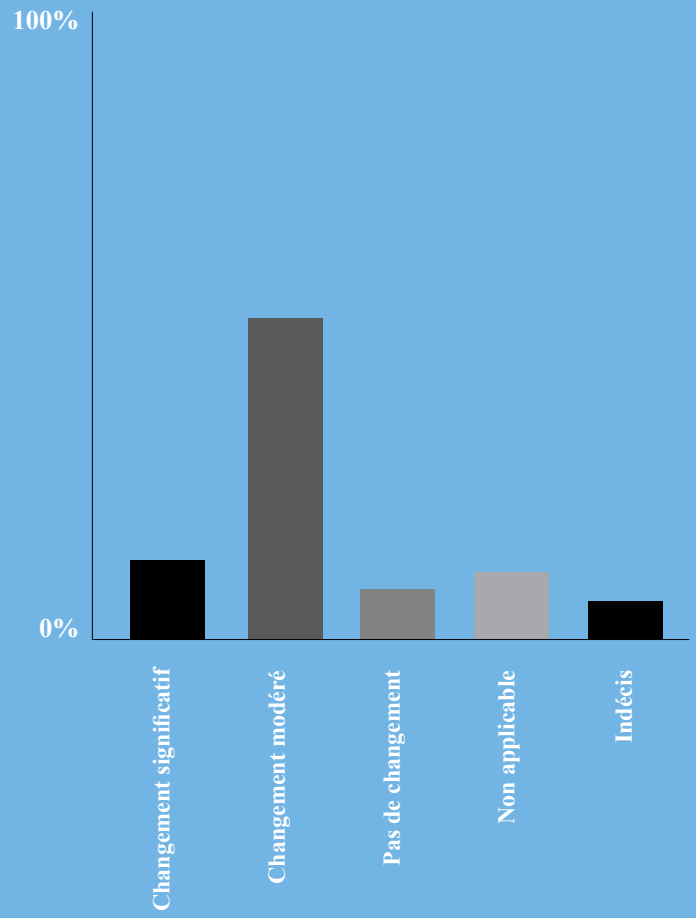
« **Habituellement**, les auditeurs ont **une formation en comptabilité**. Aujourd'hui, dans mon équipe, j'ai beaucoup trop de personnes qui **comprennent bien la comptabilité,** au détriment des compétences liées aux **technologies** par exemple. Les activités bancaires sont de plus en plus liées à la modélisation. Non seulement les modèles de **capital réglementaire**, mais aussi **des outils quantitatifs** et des modèles d'aide à la décision des clients particuliers dans leur choix de **produits d'épargne** adaptés. Les compétences pour comprendre les formules mathématiques sur lesquelles se basent ces outils et la manière dont ils fonctionnent est assez **différent des compétences traditionnelles en comptabilité.** En outre, notre banque utilise de plus en plus **d'analyses de données** dans ses opérations et l'audit interne n'est pas en reste pour la réalisation des missions ».

Responsable de l'audit interne, banque et assureur néerlandais multinational

Les comités d'audit exigent un changement

12 % des responsables de l'audit interne au Royaume-Uni indiquent que leurs comités d'audit s'attendent à ce que l'audit interne « change de manière significative », alors que 52 % indiquent qu'il faudrait des « changements modérés »

Source : Deloitte



« Quelle est votre **valeur ajoutée** en donnant un aperçu de **l'organisation** à un moment donné quand trois mois plus tard ces constats seront dépassés ? De plus en plus, il ne s'agit pas **d'auditer le présent**, mais également d'anticiper **le futur**. Pour chaque mission d'audit, nous nous demandons si la **création de valeur pour le management** sera encore valable au bout d'un an ; dans la négative, nous **passons à autre chose**. Nos objectifs d'audit sont-ils significatifs et notre approche renforce-t-elle la pertinence de l'audit ? Être sur les bons sujets mais les aborder de **manière statique** alors que ce sont des phénomènes dynamiques reléguerait **l'audit interne dans des oubliettes** ».

Responsable de l'audit interne, groupe multinational d'ingénierie et de production au Royaume-Uni

Le management devrait alors voir l'audit interne comme un conseiller digne de confiance.

Étant donné leur point de vue unique sur le contexte externe et interne, les responsables de l'audit interne peuvent également être consultés sur la capacité de l'organisation à adapter son modèle économique, à se transformer et innover face aux enjeux stratégiques. En outre, les comités pluridisciplinaires rechercheront probablement le point de vue de l'audit interne.

Pour être à valeur ajoutée, les missions d'audit devraient éviter d'offrir une revue figée d'un domaine de risques à un instant donné. L'environnement économique évolue incroyablement rapidement et les missions d'audit statiques qui ne prennent pas en considération le futur en même temps que le présent sont rapidement périmées, et par conséquent sont de moindre valeur ajoutée. Les missions d'audit sont aussi plus efficaces quand elles prennent en considération l'origine des problèmes, que ces insuffisances soient liées aux dispositifs de contrôle ou à des problématiques comportementales liées à la culture, ce qui pourrait nécessiter des compétences approfondies en analyse causale.

Cyber-risques et systèmes d'information

La principale transformation de ces dernières années est d'ordre technologique. Les auditeurs internes doivent donc avoir des compétences accrues dans le domaine du numérique afin de mieux comprendre les modalités de gestion des risques dans ce domaine et d'interpréter plus efficacement leurs constats d'audit en contribuant au renforcement de la cyber-culture des conseils et des comités.

La cybersécurité est rapidement devenue un des risques les plus sérieux auxquels sont confrontées les organisations et cela signifie que les fonctions devraient avoir des experts en audit des systèmes d'information ou avoir recours à de la co-traitance pour appréhender le niveau de préparation de l'organisation contre une attaque extérieure, de potentiels collaborateurs malveillants et d'autres vulnérabilités du système d'information, ainsi que pour avoir une vue d'ensemble de la cyber-gouvernance.

Données et analyse de données

Les organisations produisent des dépôts de données de plus en plus grands à partir de leurs opérations. A cet égard les enjeux clés pour l'audit interne sont de deux ordres. Le premier est d'aider le Conseil et la direction générale à comprendre comment ces données sont recueillies, gérées, protégées et exploitées à des fins opérationnelles. Le second est la manière d'exploiter ces données, de plus en plus nombreuses, du point de vue de l'audit interne en appliquant des outils d'analyse pour évaluer les processus, en automatisant par conséquent les missions d'audit de routine pour libérer du temps à consacrer aux domaines de risques émergents et aux projets ad hoc (voir encadré, page 32).

Culture

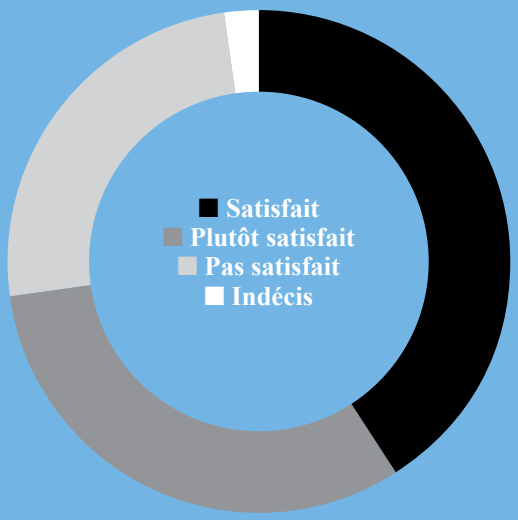
La culture organisationnelle s'est frayé un chemin au sommet des priorités de nombreux conseils (voir page 30) du fait de graves manquements d'entreprises. Les conseils souhaitent avoir l'assurance que les valeurs affirmées de l'organisation se reflètent dans le comportement des collaborateurs et que leur attitude quotidienne n'augmente pas les risques d'atteinte à la réputation. Ainsi, les compétences comportementales deviendront de plus en plus appréciées dans l'audit interne. La compréhension des indicateurs liés aux comportements individuels et collectifs ainsi que la capacité à tirer des conclusions significatives de missions d'audit plus souples qui aident les conseils et les comités d'audit à comprendre la culture des organisations et la manière dont elle est liée aux risques deviennent essentiels.

Questions clés :

- L'audit interne a-t-il effectué une analyse des écarts pour évaluer d'éventuelles lacunes de compétences ?
- Le responsable de l'audit interne comprend-il ce que sont les exigences actuelles de l'organisation en matière d'assurance, et ce qu'elles seront probablement dans le futur ? Ces attentes sont-elles en adéquation avec l'ensemble des compétences de la fonction d'audit interne ?
- La fonction d'audit interne a-t-elle envisagé le bénéfice net de l'adoption d'outils d'analyse des données ?
- Si la fonction utilise la co-traitance, ou l'externalisation pour répondre à des besoins, ces ressources ad hoc offrent-elles le niveau adéquat de connaissance, d'expertise et d'assurance ?
- La fonction a-t-elle réfléchi à de nouvelles approches plus efficientes telles que la méthode « agile » ?
- Le comité d'audit a-t-il défini ces attentes à l'égard de l'audit interne et la fonction d'audit interne est-elle à la hauteur de celles-ci ?
- La fonction d'audit interne a-t-elle mené une étude comparative de son efficacité par des évaluations externes de la qualité et est-elle à la hauteur des Principes fondamentaux de l'IIA ?
- La fonction d'audit interne a-t-elle un programme d'assurance et d'amélioration de la qualité adéquat en place pour s'assurer qu'elle progresse et évolue ?

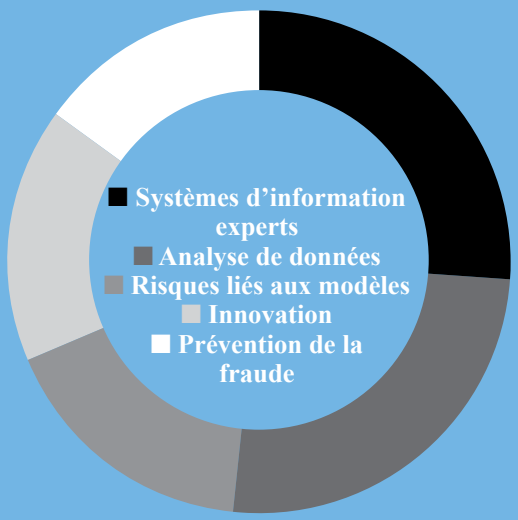
Le niveau de satisfaction des responsables de l'audit interne sur les capacités de la fonction

Source : Deloitte



Les 5 domaines en déficit de compétences selon les responsables de l'audit interne

Source : Deloitte



« Nous utilisons ce que nous appelons une approche **d'audit « agile »** pour explorer des pistes d'efficience pour améliorer plus rapidement la qualité, augmenter l'efficacité pour les **parties prenantes** de la **mission** et la communication avec nos audités.
Il y a environ un an que nous avons commencé et nous voyons déjà les bénéfices en termes de **qualité et de rapidité.**
Nous avons des « vagues » **de deux semaines**, des « mêlées », des espaces de travail collaboratifs, des **réunions régulières** pour que les équipes discutent et comprennent quels sont les domaines d'intérêt prioritaires actuels et pour **partager les connaissances** afin d'améliorer la qualité des missions d'audit ».

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

SOURCES

1. www.nccgroup.trust/uk/about-us/newsroom-and-events/press-releases/2017/april/last-years-ico-fines-would-soar-to-69-million-post-gdpr/

2. www.veritas.com/news-releases/2017-07-25-veritas-study-organizations-worldwide-mistakenly-believe-they-are-gdpr-compliant

3. www.pwc.com/us/en/risk-assurance/risk-in-review-study.html

4. https://jwg-it.eu/90-of-buy-side-firms-are-at-risk-of-non-compliance-by-mifid-ii-deadline-jwg-survey-finds/

5. https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2017.html

6. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-beps-full-survey-results-august-2017.pdf

7. www.strategyand.pwc.com/media/file/2016-Global-Innovation-1000-Fact-Pack.pdf

8. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/adapting-your-board-to-the-digital-age

9. www.paconsulting.com/insights/survey-on-innovation-for-peak-performance/

10. www.idc.com/getdoc.jsp?containerId=prUS41826116

11. economia.icaew.com/en/news/july-2017/two-thirds-of-uk-businesses-have-no-brexit-plans

12. project28.eu/opinions-2017/

13. www.uschamberfoundation.org/reports/millennial-generation-research-review

14. www.cebglobal.com/human-resources/millenial-talent.html

15. www.accenture.com/gb-en/insight-strategic-workforce-planning

16. https://www.thomsonreuters.com/en/press-releases/2017/march/thomson-reuters-survey-automation-will-change-businesses-for-better.html

17. www.hays-index.com/wp-content/uploads/2016/09/Hays-GSI-Report-2016.pdf