DOCUMENT DE RÉFLEXION

10 SUJETS INCONTOURNABLES POUR LE PLAN D'AUDIT INTERNE 2017

The Institute of Internal Auditors
France
Italy
Spain

SOMMAIRE

Remerciements

De nombreuses personnes ont contribué à la préparation de ce document. Nous souhaiterions remercier tout particulièrement les responsables de l'audit interne des différents secteurs (banque, assurance, chimie, énergie, secteur public, distribution et bâtiment) qui nous ont fait part de leur vision et de leur opinion sur les enjeux à venir pour notre profession.

PROLOGUE

Les opportunités comme les risques changent constamment, à mesure qu'évoluent les organisations et leur environnement. Anticiper les conséquences de ces risques et opportunités, ainsi que leurs ramifications, peut se révéler difficile.

L'objectif de cette étude est de catégoriser ces risques et opportunités, et de proposer des mesures adaptées pour leur prise en compte par les responsables de l'audit interne. Loin d'un cadre statique, c'est une base de discussion avec nos membres, un outil à leur disposition pour comprendre les prochains défis à relever au sein de notre profession.

Afin d'en garantir la pertinence, nous nous sommes appuyés sur différentes sources d'information, notamment des rapports publiés par des institutions et cabinets de conseil internationaux, ainsi que sur des entretiens avec des responsables de l'audit interne à travers l'Europe.

Ce document a été produit par l'IFACI, l'IIA Italie, l'IIA Espagne, avec le soutien du Chartered Institute of Internal Auditors (Irlande et Royaume-Uni).

A travers les échanges que nous aurons avec vous, et en réponse à l'évolution de l'environnement économique, nous publierons régulièrement des mises à jour de ces incontournables.

Nous reviendrons donc vers vous rapidement pour lancer cette conversation et serons ravis de recueillir vos commentaires et vos réactions.

SUJET 1

GÉOPOLITIQUE

Certains des risques les plus préoccupants, pour toutes les organisations nationales et internationales, sont de nature géopolitique.
Certaines organisations peuvent juger que ce risque est trop complexe pour être traité en interne. Pourtant toute entreprise qui exerce son activité en dehors de son pays doit faire preuve d'une solide compréhension de la géopolitique.
Nous vivons dans un monde volatile, incertain, complexe et ambigu (ou VUCA), selon l'acronyme inventé par l'armée américaine au début des années 1990, et qui conserve toute sa valeur aujourd'hui.

EN JUIN 2016, LA BANQUE MONDIALE a publié des Perspectives économiques mondiales qui présente son évaluation des risques et divergences actuels. Les risques ainsi définis sont les mêmes que ceux qui avaient été identifiés dans le même rapport 25 ans auparavant :

« Aujourd'hui, des incertitudes croissantes provenant de directions différentes, mais connexes, présagent de difficultés à venir […] Pris isolément, aucun de ces sombres nuages économiques ne serait suffisant pour obscurcir les perspectives de l'économie mondiale. Ensemble, néanmoins, ils prouvent que l'économie mondiale s'apprête à affronter une période de turbulences à court terme.

[…] L'impact des facteurs extérieurs sur les pays en développement dépendra fortement de la façon dont chaque pays fera face à de tels risques. Les politiques mises en œuvre dans les pays industrialisés devront tenir compte des préoccupations des pays "émergents et en développement" et les aider à renouer avec une croissance dynamique. Ce point semble

particulièrement important pour les pays à bas revenus qui disposent d'un nombre limité d'options stratégiques en matière de développement durable ».[1]

L'Asie et la course à la compétitivité

Avec la mondialisation, les pays coopèrent et échangent plus que jamais des biens et des services. Ce qui est source de nombreux avantages, mais entraîne également plusieurs inconvénients difficiles à gérer.

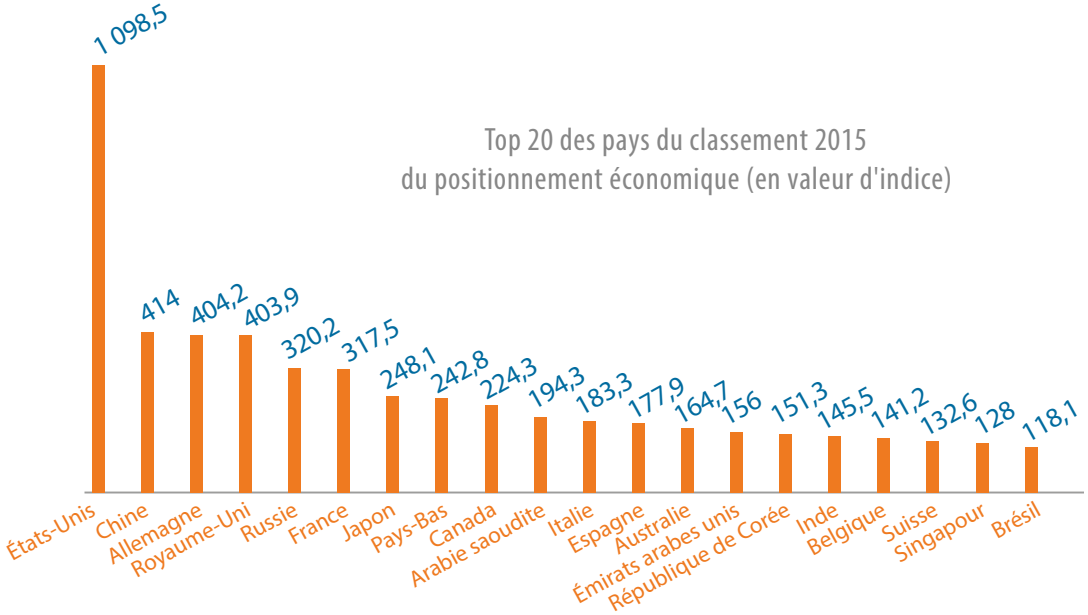
Ainsi, l'arrivée de quatre milliards d'Asiatiques sur le marché du travail a eu des conséquences dans le monde entier, et s'est traduit par d'importantes modifications en termes de centre de production et par une hausse sans précédent de compétitivité. De nombreuses organisations ont ainsi été laissées pour compte faute d'avoir réussi leur développement international.

L'édition 2016 de l'**Indice Elcano Global Presence** (fondé sur une enquête menée en 2015 auprès d'experts internationaux) classe 90 pays en fonction de leur positionnement géopolitique et économique. [2]

Cette année, l'étude met en lumière le positionnement de la Chine en deuxième place du classement, la stagnation du processus de mondialisation et l'impact de l'effondrement du prix des matières premières sur les économies émergentes.

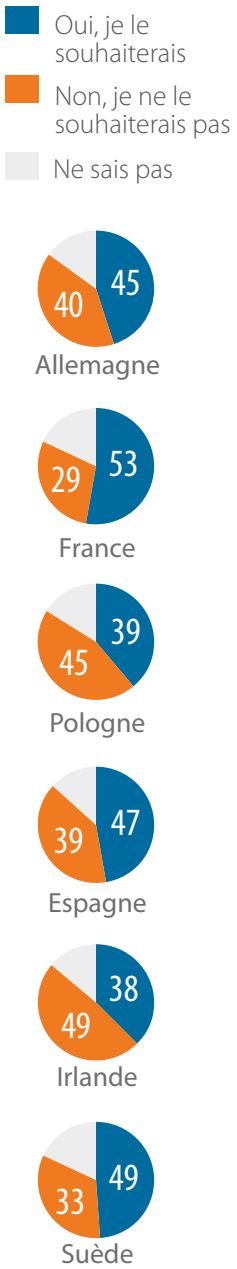
Ces facteurs, ainsi que de nombreux autres, se traduisent par un accroissement des risques et une plus forte exposition à ces risques dans des zones géographiques que nous n'avions pas anticipés, d'où une difficulté accrue à en quantifier l'impact économique sur l'organisation.

Ces facteurs, ainsi que de nombreux autres, se traduisent par un accroissement des risques et une plus forte exposition à ces risques dans des zones géographiques que nous n'avions pas anticipés, d'où une difficulté accrue à en quantifier l'impact économique sur l'organisation



Source :
Real Instituto Elcano

Souhaiteriez-vous que votre pays organise un référendum similaire à celui qui s'est tenu au Royaume-Uni ? (%)



Source : Université d'Édimbourg

Europe : une fracture aggravée par le *Brexit* ?

Dans le cas de l'Europe, région relativement stable et sûre, la situation a également évolué au cours des dernières années.

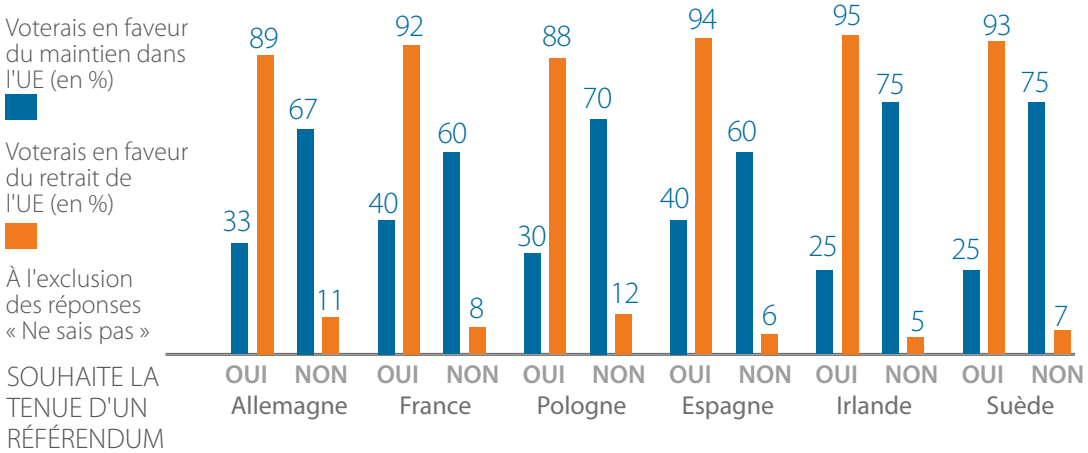
La décision prise par le Royaume-Uni de quitter l'Union européenne *(Brexit)* a surpris de nombreuses organisations. Le projet européen semble remis en cause, suite à la multiplication des crises non résolues de manière satisfaisante au sein de l'Union, et le *Brexit* jette le doute sur la validité du modèle européen dans son ensemble.

Un effet de contagion est redouté, et certaines études comme *The view from the continent: What people in other member states think about the UK's EU referendum,* conduite en juin 2016 par l'Université d'Édimbourg[3], donnent des chiffres alarmants. Ainsi, 53 % des Français souhaitent la tenue d'un référendum pour savoir si le pays doit rester ou non dans l'Union européenne, et Marine Le Pen s'est déjà engagée à l'organiser si elle remporte les élections présidentielles en 2017. Les Français sont talonnés dans ce sondage par les Suédois, les Espagnols et les Allemands, dont respectivement 49 %, 47 % et 45 % partagent la même opinion.

La crise de l'euro a mis en évidence des visions opposées entre le Nord (pays créditeurs) et le Sud (pays débiteurs), et la crise des réfugiés a créé une fracture entre l'est et l'ouest de l'Europe. Le coup d'État échoué en Turquie et les attaques djihadistes dans différents pays européens ont pesé sur les marchés boursiers et sur différents secteurs de l'économie, en particulier sur le tourisme. Selon les estimations du Ministère français des Affaires étrangères, Paris aurait perdu un million de touristes et un milliard d'euros au cours du premier semestre 2016 en raison des récentes attaques terroristes. [4]

Cette fragilité de l'Europe est à l'origine de la publication, en juin 2016, d'une Stratégie globale pour la politique étrangère et de sécurité de l'Union européenne. L'instabilité

Préférences en cas de tenue d'un référendum sur le maintien de l'adhésion de votre pays à l'UE, selon que vous souhaitez ou non qu'un tel référendum soit organisé dans votre pays (en %).



politique se traduit en effet par une fuite de capitaux et par un manque d'attractivité pour les investisseurs. [5]

Principaux facteurs à intégrer dans la cartographie des risques

Les risques géopolitiques conditionnent l'expansion internationale, la poursuite des opérations dans un pays et la réévaluation des risques de suspension d'un investissement. Ils doivent par conséquent être correctement identifiés et gérés.

Les risques géopolitiques suivants peuvent être présents dans toute cartographie des risques :

Risque politique. Les changements de gouvernement, l'instauration d'une dictature, les nationalisations, les conflits armés et les sanctions commerciales sont autant de risques qui doivent être pris en compte par les organisations qui cherchent à s'implanter dans un pays donné.

Risque réglementaire. Sujet particulièrement sensible pour les parties prenantes de l'audit interne. L'extrême complexité de ce risque, en raison des réglementations spécifiques à chaque secteur ou marché du travail et en constante évolution signifie que les organisations doivent se doter de ressources spécialisées.

Risque fiscal. L'organisation doit non seulement se conformer aux obligations fiscales imposées par la Loi, mais doit également veiller à son image pour ce qui est de l'optimisation fiscale. En effet, une telle stratégie peut avoir des répercussions négatives sur différentes parties prenantes et peut entraîner un recul des ventes, voire la perte de clients.

On peut citer comme exemple récent à cet égard, l'opinion de la Commission européenne, selon laquelle Apple aurait bénéficié d'avantages fiscaux illégaux accordés par l'Irlande en 2003 et 2004. Apple a été contraint de verser rétroactivement toutes les sommes dues, ainsi que les intérêts correspondants, soit un montant estimé à plus de 13 milliards d'euros. L'Irlande pourrait faire appel de la sanction, et le paiement de l'amende remettrait en cause la légalité de ces avantages fiscaux, de même que ceux accordés à d'autres sociétés.

Le *Brexit* jette le doute sur la validité du modèle européen dans son ensemble

Avec le soutien de la Commission sur ce point, il est possible que les pays décident d'enquêter individuellement sur les taxes dues par telle ou telle organisation. C'est déjà le cas du Portugal qui a également lancé le débat de la révision de la politique fiscale européenne et de la définition des pouvoirs des États membres en la matière.

Risque de change. La dévaluation ou l'appréciation d'une monnaie a des répercussions importantes sur les résultats, en particulier pour ce qui est des exportations et des importations. La dévaluation d'une monnaie pèse également sur les marges voire, selon le poids de la filiale par rapport à la société mère, sur le résultat consolidé.

Risque de liquidité. Toute organisation ou investisseur international peut avoir besoin d'accroître ses liquidités à un moment donné en cédant ses investissements. Toute restriction imposée par le pays à cet égard peut engendrer un risque important.

Risques juridiques. L'indépendance du système judiciaire est incertaine dans de nombreux pays, de même que son efficacité. L'ouverture d'une procédure dans ces

pays peut par conséquent se révéler lent et pas toujours équitable.

Par exemple, en Espagne et en Italie, outre le risque de sanctions administratives, la responsabilité pénale d'une entreprise peut être engagée avec un risque de dépôt de bilan et, dans les cas les plus extrêmes, une poursuite judiciaires des dirigeants.

Risques de corruption. Bien que des réglementations visent à limiter autant que possible ce risque, il est bien réel dans de nombreux pays faute d'engagement politique et l'absence de déontologie chez les fonctionnaires et les salariés du secteur privé.

Risques énergétiques, risques liés aux matières premières et à l'approvisionnement. La dépendance énergétique d'un pays ou l'absence de matières premières constitue un enjeu de tout premier ordre. L'Europe, en tant que principal consommateur de gaz en provenance de Russie est à cet égard un bon exemple. Ainsi, un tiers des besoins en Europe sont couverts par le gaz d'origine russe. La moitié de ces importations de gaz transitent par l'Ukraine, qui est en conflit avec la Russie suite à l'annexion de la Crimée. Dans certains pays, comme la Finlande, les États baltes et la République tchèque, les importations de gaz représentent un quart de la consommation énergétique totale.

Le prix constitue un autre facteur décisif. La tourmente économique provoquée par la chute du prix du baril de brut, au Venezuela par exemple, est considérable parce que son économie dépend des recettes tirées de cette source énergétique. La Russie rencontre aussi des difficultés et a élaboré son budget pour 2016 en se fondant sur un prix de 50 dollars par baril.

Le responsable de l'audit interne doit évaluer l'impact de ces risques sur l'organisation en effectuant des tests de résistance pour différents scénarios et contribuer aux efforts de la direction générale concernant la continuité d'activité et les stratégies d'investissement

Rôle du responsable de l'audit interne face à ces risques

Toutes ces variables étant interconnectées, complexes et volatiles, le **responsable de l'audit interne** doit évaluer leurs impacts sur l'organisation en effectuant des tests de résistance pour différents scénarios et contribuer aux efforts de la direction générale concernant la continuité d'activité et les stratégies d'investissement.

Dans le document *«Perspectives-internationales - Risques géopolitiques : comment y faire face ?»*, publié en mai 2015, l'IIA considère qu'il est de la responsabilité de l'audit interne de donner une assurance sur la capacité de l'organisation à anticiper les risques géostratégiques et de la conseiller en la matière.

Le responsable de l'audit interne détermine dans quelle mesure ces risques sont susceptibles de peser sur les objectifs. À cette fin, il est recommandé que la fonction d'audit interne soit représentée dans les zones qu'elle souhaite évaluer afin d'acquérir une connaissance suffisante et une expérience locale.

Par ailleurs, comme indiqué par Ernesto Martinez, Président d'IIA Espagne, dans son article intitulé *«El imperativo de la Resiliencia»,* les entreprises doivent poursuivre leurs efforts de recherche-développement, afin d'être résilientes au changement et de contribuer à leur propre stabilité.

Le facteur qui déterminera l'impact final de ces risques sur les organisations sera le système mis en place par chacune d'entre elles pour les maitriser et les gérer. L'audit interne doit par conséquent contribuer au renforcement de ces deux piliers fondamentaux.

SUJET 2

GOUVERNANCE

Les événements de ces dernières années ont clairement montré le caractère crucial de la surveillance de la gouvernance dans une organisation.
La qualité de la gouvernance est directement corrélée à la valeur attribuée à l'organisation par la société et les investisseurs. Ainsi, les bénéfices à court terme et les aspects financiers ne sont plus les seuls à être pris en compte.
La plupart des problèmes rencontrés dans les organisations sont liés à des défaillances de la gouvernance que l'audit interne a rarement été à même d'identifier.

La définition même de l'audit interne souligne sa contribution à l'amélioration des processus de gestion des risques, de contrôle et de gouvernance, mais les auditeurs internes n'ont jamais été à l'aise avec ce dernier processus.

La gouvernance est définit dans le glossaire des Normes internationales comme: *« le dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloter les activités de l'organisation en vue de réaliser ses objectifs. »*

De nombreux scandales dans différentes régions et différents types d'organisations mettent en cause la gouvernance.

En 2012, JPMorgan Chase manquait d'administrateurs suffisamment experts dans ces comités des risques, mais cette lacune n'a été corrigée qu'après les pertes de six milliards de dollars provoquées par le trader Bruno Iksil.

Au Brésil, il a fallu attendre que des centaines de millions de dollars aient disparu dans les poches des collaborateurs, des sous-traitants et des politiciens, parmi lesquelles la Présidente Dilma Rousseff elle-même, pour que Petrobras soit poursuivi pour une affaire de pots de vin et de blanchiment d'argent. Plus de quarante politiciens sont ainsi concernés par cet énorme scandale.

L'une des affaires les plus connues en Espagne est celle des « cartes noires »

concernant Caja Madrid (qui a depuis disparu). Ces cartes bancaires ont été distribuées à 86 membres du Conseil et dirigeants de la banque, qui ont réussi à faire passer ainsi pas moins de 15 millions d'euros en frais personnels.

Il est essentiel de discuter avec d'autres personnes à des postes clés de gouvernance au sein de l'organisation afin de préciser l'analyse du responsable de l'audit interne

Rôle du responsable de l'audit interne face à ces risques

On estime généralement que la gouvernance ne concerne que les entreprises cotées, alors que les entreprises non cotées en ont tout autant besoin.

En s'intéressant à ce sujet, le responsable de l'audit interne touche du doigt des points extrêmement sensibles (transparence, rémunérations, etc.) et, le plus souvent, ces questions confidentielles (telles que le plan stratégique) ne sont pas divulguées aux autres collaborateurs.

Le responsable de l'audit interne doit en particulier veiller à fournir aux membres du Conseil des garanties en matière de *due diligence* dans le cadre de leurs responsabilités de suivi des systèmes de gouvernance, de gestion des risques et de contrôle et de surveillance de la mise en œuvre des décisions opérationnelles conformément aux lignes directrices applicables.

Une mission d'audit interne de la gouvernance nécessite un positionnement adéquat du responsable de l'audit interne au sein de l'organisation. Un positionnement qui évite les restrictions ou les limitations d'accès aux données ou aux ressources, et qui renforce le soutien du Comité d'audit.

Le responsable de l'audit interne peut notamment évaluer les aspects suivants :

La structure et les activités des organes de gouvernance, les questions de diversité, de transparence, les rattachements et la répartition des responsabilités, de même que leur composition optimale en termes de connaissances, de compétences et d'expertises. À cet égard, certains régulateurs exigent la production et le suivi d'une « cartographie de la gouvernance ».

La *Norme* IIA 2110 est entièrement consacrée à la gouvernance, et selon le guide de mise en œuvre correspondant, il est nécessaire de discuter avec d'autres personnes à des postes clés de gouvernance au sein de l'organisation afin de préciser l'analyse du responsable de l'audit interne concernant les processus spécifiques mis en place au sein de l'organisation et les dispositifs de maîtrise existants. Le Président du Conseil (ou pour le secteur public, l'élu ou l'officiel nommé) fait partie de ces rôles clés, de même que les auditeurs externes ou encore le responsable de la déontologie, le responsable des ressources humaines et le responsable de la gestion des risques.

Dans le cas des entreprises cotées, l'évaluation du processus d'organisation des assemblées générales des actionnaires est extrêmement importante parce que c'est le premier maillon de la chaîne de gouvernance.

Le Code de déontologie que devrait posséder le Conseil de même que le Code de conduite contenant toutes les obligations à respecter.

Les mesures destinées à éviter les conflits d'intérêt, de même que les programmes visant à détecter toute utilisation d'informations confidentielles, font partie des aspects à suivre constamment.

La surveillance de l'engagement de responsabilité lié aux infractions commises par des cadres ou des dirigeants et de la mise en place de mécanismes de communication efficaces.

Le plan stratégique pour être en phase avec l'activité, prendre en compte les politiques concernant les nouveaux marchés, produits et services.

La gouvernance des systèmes d'information, qui doit être en phase avec les objectifs opérationnels, la gestion de la qualité des données, la sécurité. Il convient de s'assurer que ces informations sont effectivement adressées aux membres du Conseil pour des prises de décision efficaces.

Le suivi de la performance par le Conseil, ses comités et la direction générale. Cette surveillance devrait être évaluée au moins une fois par an.

La conception et la pertinence des politiques de rémunération doivent être réévaluées régulièrement, de même que le fonctionnement du Comité des rémunérations chargé de définir la rémunération des dirigeants.

Le plan de succession constitue également un aspect important car la planification du remplacement des administrateurs et des dirigeants suscite la confiance les actionnaires. Ce plan témoigne de la capacité de l'organisation à faire face aux imprévus et de son aptitude à garder constamment un œil sur le *business model*.

L'évaluation des fonctions de gestion des risques, de contrôle et de conformité doit être effective et couvrir leur niveau de coordination, notamment, lorsque cela est possible, à travers l'examen de la cartographie des prestataires d'assurance.

L'audit interne occupe une place de premier plan pour l'évaluation de la gouvernance, et tout doit être mis en œuvre pour orienter ses travaux vers les aspects les plus critiques pour l'organisation.

Le plan de succession constitue un aspect important car la planification du remplacement des administrateurs et des dirigeants suscite la confiance les actionnaires

SUJET 3

CULTURE DE L'ORGANISATION

La culture de l'organisation est devenue une question d'importance stratégique. Souvent considérée jusqu'ici comme un concept abstrait, elle amène aujourd'hui de nombreuses entreprises à gérer des indicateurs sur les talents, la réputation, la qualité de service, voire les résultats financiers. La culture de l'organisation peut, lorsqu'elle est bien gérée, devenir un atout, qui permet à l'organisation de se démarquer de ses concurrents.

Néanmoins, évaluer correctement la culture d'une organisation n'est pas une tâche aisée.

La difficulté réside en premier lieu dans le fait qu'en raison des structures complexes mises en place dans de nombreuses organisations, bien souvent plusieurs cultures coexistent. C'est particulièrement le cas des organisations qui se sont développées par des acquisitions successives.

La culture de l'organisation est un concept complexe à quantifier et à objectiver. C'est à travers ce qu'ils voient ou entendent au sein de l'organisation que les individus en perçoivent la culture, et c'est pourquoi celle-ci dépend des valeurs et des comportements.

Un leader hors du commun se cache généralement derrière une solide culture d'organisation (et il s'agit souvent du fondateur lui-même). De tels leaders sont reconnus en tant que décideurs et bons communicants, capables de véhiculer leurs valeurs personnelles et de les diffuser dans l'ensemble de l'organisation. Ces caractéristiques sont un atout lorsque l'orientation donnée est reconnue, mais présente de nombreux inconvénients lorsque les valeurs ne sont pas celles attendues.

Les variables culturelles

Gómez L. et Belkin D. évoquent sept composantes qui rendent compte de l'essence de la culture d'une organisation. Ces sept dimensions sont les suivantes :

Innovation et acceptation des risques : autrement dit, dans quelle mesure les collaborateurs sont incités à être innovants et à prendre des risques.

Sens du détail : dans quelle mesure il est attendu des collaborateurs de faire preuve de précision, d'analyse et d'attention aux détails.

Focalisation sur les résultats: dans quelle mesure les managers centrent leur attention sur les résultats et les effets, plutôt que sur les techniques et processus par lesquels ces résultats ont été obtenus.

L'attention accordée aux collaborateurs: dans quelle mesure les décisions administratives tiennent compte de l'incidence des résultats sur les hommes et les femmes qui constituent l'organisation.

Esprit d'équipe : dans quelle mesure les activités professionnelles sont organisées autour des équipes, plutôt qu'autour des individus.

Combativité : dans quelle mesure les collaborateurs font preuve de pugnacité et d'esprit de compétition, plutôt que d'être dociles et complaisants.

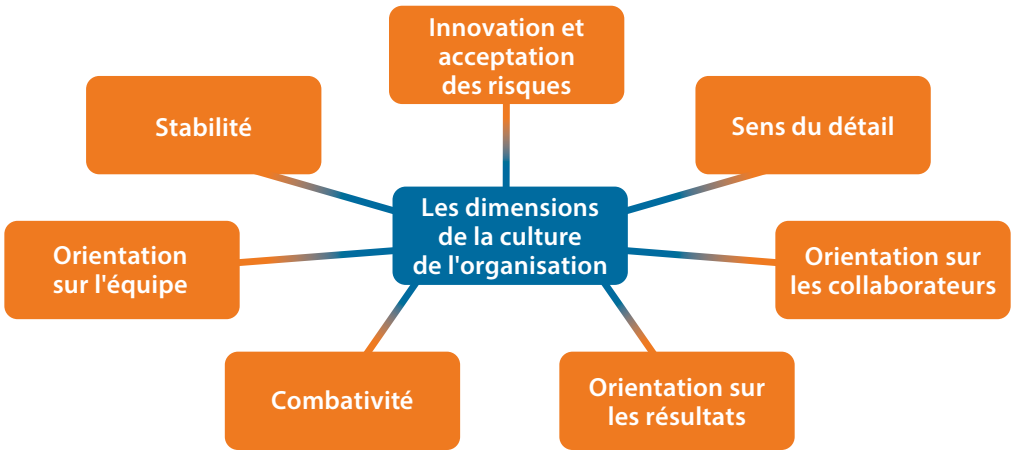
Stabilité : la mesure dans laquelle les activités entreprises par l'organisation favorisent le maintien du statu quo.

L'acceptation des risques est une composante importante de la culture de l'organisation. Certaines organisations ont une forte appétence pour le risque et se distinguent par leur dynamisme, ce qui ne met pas toujours l'auditeur interne très à l'aise. D'autres organisations, sont tellement atones qu'elles sont incapables de s'adapter aux changements et finissent par disparaitre.

On peut citer l'exemple d'une entreprise comme Kodak, qui n'a pas été capable de se réinventer lors de l'avènement des nouvelles technologies.

Kodak était connu pour être adverse aux risques. L'entreprise avait toutefois omis de

La culture d'une organisation peut autoriser certaines conduites et en interdire d'autres, ce qui induit des comportements spécifiques



prendre en compte le risque inhérent au refus du changement dans un environnement en mutation.

La culture d'une organisation peut autoriser certaines conduites et en interdire d'autres, ce qui induit des comportements spécifiques.

Ce ne sont pas forcément les collaborateurs les plus hauts placés qui ont la plus forte influence sur la culture de l'organisation

Il y a quelques années encore, on ne considérait pas que les risques liés à la culture nécessitaient une surveillance ou la mise en place de dispositifs de contrôle. Cependant, à l'instar d'autres risques, les risques liés à la culture ont commencé à être gérés de façon plus formelle dans le secteur financier et a été mis en avant par les autorités de régulation et de supervision.

C'est ce qu'ont fait, par exemple au Royaume-Uni, la *Financial Conduct Authority* (FCA) et la *Prudential Regulation Authority* (PRA), qui ont publié une série d'instructions visant à confirmer la nécessité de renforcer la responsabilité individuelle dans le secteur financier. Ces normes définissent le régime applicable aux cadres dirigeants et à la certification, ainsi que les nouvelles règles de conduite à mettre en œuvre.

En juin 2013, la *Parliamentary Commission on Banking Standards* (PCBS) a publié un rapport intitulé *Changing Banking for Good*, qui définit des recommandations d'ordre législatif et autre visant à améliorer la déontologie et la culture du secteur bancaire au Royaume-Uni. Prochainement (le 7 mars 2017 exactement), ces nouvelles règles de conduite s'appliqueront à l'ensemble des collaborateurs à travers le secteur bancaire.

Les autorités de régulation cherchent à travers de telles mesures à renforcer l'un des aspects les plus importants d'une bonne culture d'organisation : la déontologie.

Le rôle du responsable de l'audit interne relatif à la culture de l'organisation

Lorsque le responsable de l'audit interne lance une mission sur la culture de l'organisation, il lui incombe de déterminer les attentes de l'ensemble des parties prenantes et si la culture est adaptée et contribue à la réalisation des objectifs de l'organisation.

Lorsque des faiblesses sont identifiées, il doit conseiller le management sur la façon dont certains aspects doivent être redéfinis, tout en étant conscient que l'impact de ces recommandations sur une culture solidement ancrée n'est pas immédiat.

En outre, il convient d'être vigilant lors de la communication de ces mesures aux autres collaborateurs et d'évaluer l'impact que de telles actions peuvent avoir sur la culture de l'organisation.

Carly Fiorina, par exemple, n'a pas réussi à faire ses preuves en tant que PDG de Hewlett-Packard parce qu'elle a essayé d'imposer une culture centrée sur les ventes à une organisation dirigée par des ingénieurs.

D'une manière générale, les plans d'actions doivent être développés depuis le sommet de la hiérarchie parce que le management doit être le premier à donner l'exemple et à relayer les messages qui définissent la conduite attendue.

L'*Institute for Business Ethics* a publié un document intitulé *Checking culture: a new*

role of internal audit.[5.1], selon lequel les auditeurs internes ne peuvent pas et ne doivent pas travailler isolément. Le responsable de l'audit interne peut recevoir une aide précieuse d'autres personnes au sein de l'organisation, telles que le directeur de la conformité et de la déontologie ou le directeur des ressources humaines.

Ce ne sont pas forcément les collaborateurs les plus hauts placés qui ont la plus forte influence sur la culture de l'organisation. Autrement dit, il convient de déterminer quels sont ceux qui ont le plus d'emprise sur leurs collègues grâce à leur autorité naturelle.

En outre, le responsable de l'audit interne doit être conscient qu'aucune action n'aura de résultat immédiat, ce qui signifie qu'il devra constamment suivre les changements qui se produisent et s'assurer que les effets obtenus sont bien ceux attendus.

Il convient de souligner que le responsable de l'audit interne doit également évaluer la culture de son propre service, à savoir principalement son leadership, ses méthodes de communication et la façon dont il est perçu.

De nombreuses organisations obtiennent un *feedback* par le biais des enquêtes d'opinion, dans lesquelles sont évalués différents aspects de la culture de l'organisation y compris la perception de l'audit interne.

Le rapport 2016 intitulé *Organisational Culture, evolving approaches to embedding and assurance* du *Chartered Institute of Internal Auditors* (Irlande et Royaume-Uni), met en lumière la complexité de mise en œuvre de ce type de missions et la préparation nécessaire de la part de l'audit interne et du comité d'audit.

Les caractéristiques de ces revues ne sont pas les mêmes que celles d'une mission classique, exception faite de la revue des procédures, politiques et processus, et des zones de flou sont inévitables en raison des divers critères qu'ils faudra définir avec les personnes concernées.

SUJET 4

CONFORMITÉ

Le rôle de la conformité s'est considérablement développé dans la plupart des organisations sous l'effet de la mondialisation et de leur propre développement international. En France, par exemple, le responsable conformité et les responsables du contrôle interne figurent parmi les sept métiers les plus porteurs du moment.[6]

Ce processus s'est accentué ces dernières années après l'éclatement d'un certain nombre de scandales dans le monde entier. Les régulateurs ont souvent eu à intervenir afin de protéger les parties prenantes et l'intérêt général, contribuant ainsi à la complexification de l'environnement législatif international.

Le nouveau Règlement général sur la protection des données (GDPR) (règlement (UE) n°2016/679), qui entrera en vigueur en mai 2018, prévoit que les entreprises qui fournissent des services aux citoyens de l'Union européenne peuvent faire l'objet d'amendes allant jusqu'à 20 millions d'euros ou 4 % de leur chiffre d'affaires mondial (le montant le plus élevé étant retenu) si elles ne protègent pas et/ou ne traitent pas correctement les données.

Le 19 août 2016, le *New York Financial Services Department* a infligé une amende de 180 millions de dollars à la Mega International Commercial Bank of Taiwan pour violation de la législation relative au blanchiment de capitaux de l'État de New York et lui a imposé de désigner un contrôleur indépendant.[7] L'amende a été définie à l'issue d'un consentement mutuel avec le régulateur, aux termes duquel la banque acceptait d'une part de prendre des mesures immédiates pour pallier ses manquements en matière de conformité, et notamment de nommer un contrôleur indépendant chargé de remédier aux graves insuffisances du programme de conformité, et d'autre part de mettre en œuvre des contrôles pour lutter contre le blanchiment de capitaux.

Ainsi, les responsabilités se sont vues renforcées et, désormais, la responsabilité pénale peut être engagée. Des non-conformités peuvent conduire une société à déposer le bilan et avoir des répercussions bien au-delà du contexte local : un tel événement peut affecter jusqu'à la société mère, dont la réputation risque alors de se trouver considérablement entachée.

Au Royaume-Uni, par exemple, toute personne ayant enfreint la législation anti-corruption est passible d'une peine allant jusqu'à 10 ans de prison et/ou, pour les entreprises jugées coupables d'une telle infraction, d'une amende illimitée.

Aux États-Unis, tout contrevenant à la loi sur la corruption dans les transactions à l'étranger de 1977 (*Foreign Corrupt Practices Act*, FCPA) s'expose à une amende allant jusqu'à 250 000 dollars, ainsi qu'à une peine de prison allant jusqu'à 5 ans, s'il est reconnu coupable. Une entreprise jugée coupable d'une infraction à cette loi est passible d'une amende pouvant atteindre jusqu'à 2 millions de dollars.

En Espagne, la loi organique n°5/2010 du 22 juin, votée en 2010 (et réformée par la loi organique n°1/2015), introduit le concept de responsabilité pénale pour les entités juridiques dans le système judiciaire. Depuis lors, le « contrôle approprié » *(debido control)* est devenu un enjeu, de même que la nécessité de mettre en œuvre des programmes de conformité pour créer des mécanismes de contrôle agissant comme cause d'exonération.

En France, la loi n°2016-1691 du 09 décembre 2016 dite loi « Sapin 2 » renforce la lutte contre la corruption.

Dans certains secteurs, tels la banque et l'assurance, la fonction conformité est déjà fortement développée en raison des exigences du régulateur.

Le dispositif de conformité doit être en phase avec le modèle de gouvernance de l'entreprise et bénéficier de mécanismes adéquats de séparation des pouvoirs, des responsabilités et des processus de prise de décision. Il devrait bénéficier d'un soutien approprié de la part du management, ainsi que de solutions technologiques de pointe et de professionnels compétents, capables d'accomplir efficacement leur rôle.

Le dispositif de conformité doit être en phase avec le modèle de gouvernance de l'entreprise et bénéficier de mécanismes adéquats de séparation des pouvoirs, des responsabilités et des processus de prise de décision

CULTURE DE LA CONFORMITÉ

De nombreux régulateurs s'efforcent actuellement de faire évoluer la culture de la conformité dans les entreprises et de légiférer sur les nouveaux modèles d'organisation que font émerger les nouvelles technologies. Il ne s'agit pas simplement de se mettre en conformité pour le simple fait d'être en conformité.

Les régulateurs manquent de ressources pour superviser de manière exhaustive toutes les organisations. Par conséquent, ils adoptent une démarche différente, centrée sur l'autorégulation, la mise en œuvre d'une culture de l'intégrité, et le recours à des programmes déontologiques qui instaurent une confiance suffisante pour tous.

Malgré les efforts déployés, le phénomène de « cécité éthique » – concept défini par le professeur Guido Palazzo, selon lequel les priorités d'une organisation poussent ses collaborateurs à la corruption – n'est pas près de disparaître.

Il n'est pas surprenant de voir un nombre croissant d'organisations s'employer à renforcer leurs règles de gouvernance à l'échelle mondiale et dédier davantage de ressources à l'élaboration de dispositifs d'alerte. Ces dispositifs permettent

Pour une organisation, l'objectif le plus important en termes de conformité est de mener ses opérations avec intégrité

aux entreprises de détecter et de corriger les défaillances internes avant qu'elles ne soient rendues publiques, protégeant ainsi la valeur des parties concernées.

Il existe également des programmes de primes pour les lanceurs d'alerte qui collaborent avec les autorités et les aident à démasquer des cas de fraude.

Le 31 août 2016, aux États-Unis, la *Securities and Exchange Commission* (SEC) a annoncé avoir versé plus de 22 millions de dollars à un lanceur d'alerte dont les renseignements et l'aide précise lui avait permis de mettre fin à une fraude orchestrée par la société où il travaillait. Cette prime constitue le deuxième plus gros montant jamais octroyé par la SEC à un lanceur d'alerte. La récompense la plus forte, qui s'élevait à 30 millions de dollars, a été versée en 2014.

Ces primes soulignent l'importance accordée par le régulateur aux dispositifs d'alerte.

Au Royaume-Uni également, la *Financial Conduct Authority* (FCA) donne une grande importance aux lanceurs d'alerte et a publié en 2015 de nouvelles règles pour asseoir ce rôle.[8]

La France a également fait des progrès en la matière. Notamment grâce à la loi n°2016-1691 du 09 décembre 2016 dite loi « Sapin 2 » qui protège dorénavant les lanceurs d'alerte.

Pour une organisation, l'objectif le plus important en termes de conformité est de mener ses opérations avec intégrité.

La conformité n'a pas seulement pour but de protéger l'organisation et sa réputation, mais sert également à défendre les intérêts des clients, des fournisseurs, des partenaires et de toute personne entretenant des liens avec l'organisation.

LE RESPONSABLE DE L'AUDIT INTERNE : CONSEILLER STRATÉGIQUE EN MATIERE DE CONFORMITÉ

Il y a quelques années, le modèle de croissance d'une société consistait à répliquer la structure hiérarchique du siège dans chaque pays. Toutefois, l'hétérogénéité des réglementations nationales contraint fortement cette pratique.

C'est la raison pour laquelle le **responsable de la conformité (*Chief Compliance Officer - CCO*)** acquiert actuellement un rôle important en tant que conseiller stratégique de l'entreprise.

Dans une étude intitulée ***Local Compliance in Global Business. A journey through a changing landscape, BDO*** analyse les différents modèles organisationnels adoptés par les entreprises à des fins de conformité au niveau local, et les défis auxquels elles font face pour rationaliser leurs processus et garantir le respect des réglementations locales.

Dans ces cas, l'externalisation des rôles se limite généralement à la vérification du respect des réglementations existantes dans chaque pays par un prestataire local. Cependant, on constate qu'il n'existe aucune corrélation pertinente entre les risques liés à la conformité au niveau local et les mesures prises par les sociétés pour assurer à la fois le contrôle et la visibilité nécessaires au niveau du siège.

En outre, la tendance est la délocalisation de divers processus dans certaines zones géographiques (telles que l'Inde ou la Chine), ce qui permet une réduction substantielle des coûts, voire une externalisation du service.

La réalisation de tâches de *due diligence* par ces prestataires de services prend une importance extrême, compte tenu du fait que le risque réglementaire n'est pas communiqué.

Il est également important de préciser que la plupart des risques réglementaires sont transversaux (le régulateur s'intéressant à la gouvernance, à la gestion des risques, à la protection des données, à la cybersécurité, etc.), c'est-à-dire qu'ils concernent différents services. Une coordination adaptée entre les différents domaines de supervision devient donc nécessaire.

Le fait que l'organisation doive s'adapter aux exigences réglementaires – à travers une transformation des processus existants ou la mise en œuvre de nouveaux processus – constitue pour le responsable de l'audit interne l'occasion de s'impliquer activement en tant que conseiller.

On constate qu'il n'existe aucune corrélation pertinente entre les risques liés à la conformité au niveau local et les mesures prises par les sociétés

SUJET 5

ENVIRONNEMENT DE TRAVAIL

Un bon environnement de travail va généralement de pair avec la productivité, ce qui constitue un avantage compétitif dans un monde de plus en plus complexe. L'image que les organisations renvoient au grand public fait également partie des préoccupations : aujourd'hui, les entorses aux bonnes pratiques des affaires peuvent se retrouver instantanément étalées sur les réseaux sociaux, lesquels ont ainsi le pouvoir de faire ou de défaire une marque.

Depuis le début des années 1960, les études sur les comportements au sein des organisations soulignent combien il est difficile de dégager des principes universels applicables à des personnes différentes, qui ne travaillent pas de la même manière.

L'environnement de travail est un facteur difficile à quantifier, bien qu'il puisse être évalué *via* des enquêtes anonymes ou des entretiens auprès du personnel qui quitte l'organisation. De tels dispositifs permettent d'avoir une idée sur la perception que les collaborateurs ont de l'organisation. Pourtant, ces indicateurs clés de performance n'apparaissent que rarement sur les tableaux de bord et ne sont pas souvent remis au comité d'audit pour analyse.

Pourtant, la détérioration de l'environnement de travail représente un risque important pour l'organisation. Ce risque doit être traité efficacement car il ouvre souvent la voie à d'autres problèmes tout aussi graves.

Parmi ses conséquences négatives, on peut citer : l'incapacité des collaborateurs à s'adapter, le taux de rotation du personnel élevé, l'absentéisme, la faiblesse de l'innovation, la productivité insuffisante et les atteintes à la déontologie.

Le stress au travail – notamment causé par des temps de travail importants, l'insécurité de l'emploi ou l'absence d'équilibre entre vie privée et vie professionnelle – est responsable d'au moins 120 000 décès chaque année aux États-Unis et coûte jusqu'à 190 milliards de dollars au système de santé, selon une étude menée par deux professeurs de Stanford et un ancien doctorant de cette même université, désormais en poste à la Harvard Business School.

Si le responsable de l'audit interne a bien incorporé tous ces éléments à la revue de la direction des ressources humaines qui traite spécifiquement de ce risque, il demeure important de toujours tenir compte de l'environnement de travail comme facteur indirect lors de la revue de n'importe quel service.

Les auditeurs internes devraient toujours tenir compte de l'attitude des collaborateurs ainsi que de leurs interactions avec l'audit interne et le commanditaire de la mission.

La coexistence de différentes générations (sujet incontournable n°6) au sein de l'organisation implique une transformation radicale de la gestion d'équipe.

Les équipes ne sont plus seulement pluridisciplinaires en termes de connaissances ; elles devraient également devenir intergénérationnelles pour allier expérience et talent, ce qui peut jouer un rôle clé dans la création d'un environnement de travail adéquat.

L'une des façons de se faire une première idée de l'environnement de travail est de passer en revue les postes de travail, l'organisation de l'espace, les activités extra-professionnelles proposées, le ton des conversations et les comportements à la machine à café. Bien qu'ils puissent ne pas sembler pertinents à analyser, ces aspects informels sont extrêmement importants et peuvent receler de précieux signaux d'alerte.

En outre, la détérioration de l'environnement de travail affecte aussi directement le responsable de l'audit interne et sa manière de gérer son équipe.

Notons que le service d'audit interne est sensible à plusieurs facteurs :

- Les efforts intellectuels à fournir sont grands, du fait de la complexité et de la variété des missions d'audit, ainsi qu'en raison de la formation continue qu'il convient de suivre pour rester parfaitement à jour.

- La plupart des tâches sont assorties d'échéances très strictes que les auditeurs s'efforcent constamment de respecter, les déplacements peuvent être fréquents et les discussions avec le management sur les recommandations peuvent se dérouler dans un climat tendu.

- Si on ajoute à ces éléments la méconnaissance des collègues sur les objectifs de l'audit, la dégradation de l'environnement de travail est garantie.

Dans son service, le responsable de l'audit interne est responsable en dernier ressort d'instaurer un environnement de travail favorable qui élimine ou limite les stress et incite les auditeurs à donner le meilleur d'eux-mêmes.

Les équipes ne sont plus seulement pluridisciplinaires en termes de connaissances ; elles devraient également devenir intergénérationnelles pour allier expérience et talent, ce qui peut jouer un rôle clé dans la création d'un environnement de travail adéquat

Leadership du responsable de l'audit interne

Le responsable de l'audit interne ne devrait pas tant se préoccuper de former correctement son équipe d'un point de vue technique que se concentrer sur des aspects qualitatifs tels que la sécurité et la confiance – autant de sujets qui permettront d'améliorer l'environnement de travail

Pour réussir, il est essentiel de faire preuve d'un leadership exemplaire et de traiter chaque membre de l'équipe comme une personne à part entière et non comme une simple ressource.

Les collaborateurs devraient **se sentir impliqués par rapport aux objectifs et s'approprier les principes ou les valeurs de l'organisation,** ce qui les inciterait à se conduire de la manière souhaitée. Pour ce faire, il faut que le responsable de l'audit interne soit un expert en communication, qu'il sache comment transmettre ces valeurs et ces objectifs, et qu'il soit capable d'instaurer un environnement au sein duquel chaque personne du service – quel que soit son poste – se sente valorisée.

Le responsable de l'audit interne ne devrait pas tant se préoccuper de former correctement son équipe d'un point de vue technique que se concentrer sur des aspects qualitatifs tels que la sécurité et la confiance – autant de sujets qui permettraient d'améliorer l'environnement de travail.

Il devrait être capable de déterminer et de connaître les intérêts personnels de chaque collaborateur, ce qui suppose un bon niveau d'intelligence émotionnelle ainsi que la faculté à encourager l'implication et à veiller sur l'épanouissement des talents.

Le responsable de l'audit interne devrait tisser des liens d'amitié et de confiance à travers des entretiens en face-à-face (ou des entretiens virtuels si les collaborateurs travaillent à distance), des petits-déjeuners, ou toute autre activité qui facilite la connaissance directe des attentes des collaborateurs.

Par ailleurs, la reconnaissance d'un travail bien fait reste un facteur de motivation important. Dans ce domaine, le renforcement positif devrait jouer un rôle majeur, mais le fait pour un responsable de l'audit interne de se montrer impliqué et toujours serviable peut aussi se révéler extrêmement bénéfique.

Le responsable de l'audit interne sera amené à échanger avec la prochaine génération d'auditeurs internes (sujet incontournable n°6), dont la mentalité peut parfois différer de celle des générations qui la précèdent et qui fait preuve d'un talent et d'un charisme certains, tout en réclamant des modifications substantielles de l'organisation du travail.

La flexibilité des horaires, le télétravail ou la fixation d'objectifs sont autant d'éléments qui pousseront le service d'audit interne à se transformer.

La réduction des contraintes bureaucratiques, l'amélioration des processus et leur rationalisation la plus poussée possible, ainsi que les efforts en faveur d'une supervision accrue, favoriseront un meilleur environnement de travail.

Le responsable de l'audit interne devrait être un professionnel capable de transmettre sa passion et de veiller à ce que les auditeurs internes soient dans une démarche d'innovation et d'amélioration créatrice de valeur pour le service. Il devrait en même temps se montrer tolérant vis-à-vis de l'échec, des erreurs ou des efforts se soldant par des résultats limités.

SUJET 6

GÉRER LA PROCHAINE GÉNÉRATION

On estime que plus d'un quart de la population mondiale (27 %, l'équivalent de 2 milliards d'individus) appartient à la « génération Y » (19-35 ans) ou « millenials », et qu'un tiers (32 %, soit 2,4 milliards d'individus) fait partie de la génération suivante, connue sous le nom de « génération Z » (0-18 ans). Ces deux générations totalisent 59 % de la population mondiale et, en 2020, elles constitueront 60 % de la main-d'œuvre.

À ELLES DEUX, ces générations sont majoritaires et probablement les plus différentes des générations qui les précèdent, et leurs caractéristiques induisent des transformations sans précédent dans les organisations du monde entier.

Elles se caractérisent par leur défense de la diversité, du développement durable et de l'ouverture au monde. Elles ont grandi à une époque de véritable révolution technologique, dont elles voient l'effet dans leur vie quotidienne. Selon le Forum économique mondial de 2016, 86 % « millenials » voient les nouvelles technologies d'un œil favorable et pensent que cette évolution crée des emplois plus qu'elle n'en détruit.

Ces jeunes générations sont donc ouvertes à l'émergence de nouveaux modèles économiques, à l'instar de ceux créés par des icônes de leur époque, de jeunes hommes et femmes d'affaires comme Mark Zuckerberg, Wang Xinwen, Tavi Gevinson, Elon Musk, Robert Nayo et Maddie Robinson, qui seraient devenus multimillionnaires en s'investissant dans un projet qui les attire et auquel ils croient.

Si une organisation n'est pas capable de répondre sur-le-champ, elle court le risque de perdre des clients

Près de 55 % des 10 000 jeunes gens de la génération Z sondés par Universum se disent tentés par l'idée de créer leur propre entreprise, et ce chiffre grimpe à 75 % pour les panels interrogés au Moyen-Orient, en Europe centrale et en Europe de l'Est. Leurs principaux objectifs sont de devenir leur propre patron et d'avoir un impact sur la société.

Dans leur vie active, ce sont des professionnels non conformistes qui s'accommodent de la flexibilité de l'emploi et font passer leur qualité de vie avant leur carrière professionnelle. Parallèlement, ils sont extrêmement proactifs, ils sont force de proposition et ils ne craignent pas de soumettre des idées innovantes.

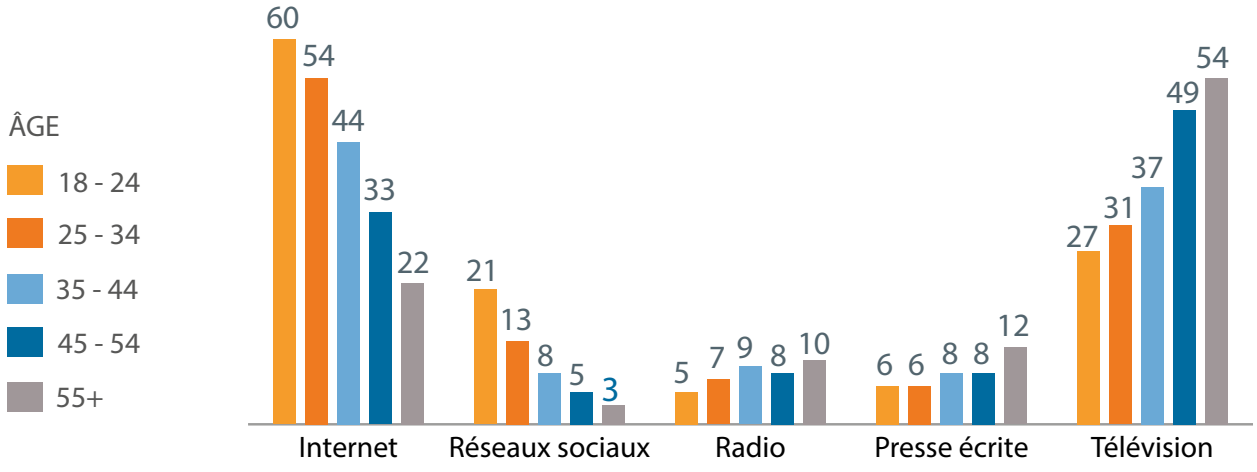
Cependant, comme le fait remarquer Rick Goings, PDG de Tupperware Brands : *« Les « millenials » veulent monter leur propre entreprise. Toutefois, si on observe leurs aptitudes, leurs compétences cognitives sont indéniables, mais il leur manque souvent d'autres qualités comme le leadership, les compétences relationnelles et l'esprit d'équipe. »*

En revanche, les générations Y et Z aiment garder contact via les smartphones, les applications et les réseaux sociaux, et, en tant que clients, ils exigent que les sociétés communiquent avec eux par ce même biais. Par exemple, Facebook déclare que les « millenials » regardent leur téléphone portable environ 150 fois par jour, contre 30 fois par jour pour le reste des adultes.

Ils sont avides d'informations, mais contrairement aux générations précédentes, ils ne privilégient pas la télévision ou la presse écrite (à travers le monde, 60 % des plus jeunes représentants de la génération Y – 16-24 ans – utilisent Internet comme principale source d'information). En outre, ils comparent des informations issues de plusieurs sources et les diffusent ensuite sur les réseaux sociaux.

En raison de leurs modes de communication et de leurs comportements, l'influence de ces générations sur la plupart des organisations est indéniable.

Principales sources d'information par cohorte démographique



Source : Université d'Oxford, institut Reuters

Ces nouveaux modes de communication ont entièrement révolutionné le secteur de la publicité, car ces générations aiment donner leur avis dès qu'elles ont acheté un produit ou bénéficié d'un service via des plateformes en ligne comme Yelp, des sites Internet, des forums ou des blogs, sur lesquels elles partagent leur expérience d'achat avec des milliers de clients potentiels.

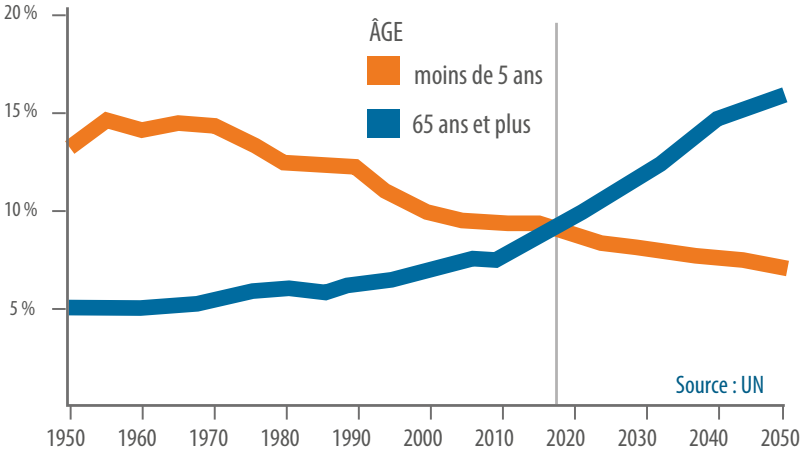
Leurs opinions sont si importantes que l'agence publicitaire Barkley déclare que 68 % de *« millenials » « ne prennent pas de décision sans en avoir discuté au préalable avec d'autres personnes »* et qu'environ 51 % d'entre eux *« font davantage confiance à des inconnus qu'à leurs amis lorsqu'ils envisagent d'effectuer un achat important ».*

Puisqu'ils sont nés et ont grandi avec la révolution numérique, ils sont habitués à une communication instantanée et se montrent donc impatients. Ainsi, si une organisation n'est pas capable de répondre sur-le-champ, elle court le risque de perdre des clients.

Le concept de « temps réel » est aujourd'hui une réalité : *« Les implications pour les marques sont fortes lorsqu'elles envisagent de s'adresser à un public qui se vante de pouvoir répondre à 40 sollicitations en une minute. »* [9]

Ces générations accordent plus d'importance à la rapidité de la réponse qu'à sa forme, car elles utilisent un langage familier et incluent des éléments tels que des émoticônes dans leur communication mobile – c'est le cas pour près de 90 % des *« millenials »,* selon le *Consumer Mobility Report 2016* de Bank of America. Leur utilisation est tellement répandue et ancrée dans la conscience de la jeunesse que le Mot de l'année 2015 du Oxford Dictionary était une émoticône (« Visage qui pleure de joie »).

Nombre de personnes âgées de plus de 65 ans par rapport au nombre d'enfants âgés de 5 ans ou moins



De nouveaux défis et leurs implications

Tant la génération Y que la génération Z se retrouvent face à un défi important du point de vue démographique en raison de la baisse des taux de natalité et de la hausse de l'espérance de vie. En 2020, pour la toute première fois de l'histoire, le nombre de personnes âgées de plus de 65 ans dépassera le nombre d'enfants âgés de 5 ans ou moins. En 2050, la génération Silver (65 ans et plus) sera passée de 885 millions à 3,4 milliards de personnes. [10]

Ces problèmes pourraient signifier l'appauvrissement des générations Y et Z par rapport à leurs parents et leurs grands-parents, avec pour corollaire des difficultés en termes de croissance économique et l'émergence d'un scénario qui nous forcera à chercher des solutions aux problèmes ayant trait à la santé, au logement, aux retraites, au marché du travail, aux finances publiques et à d'autres types de risques qui transformeront l'économie telle que nous la connaissons aujourd'hui.

L'émergence d'un scénario qui nous forcera à chercher des solutions aux problèmes ayant trait à la santé, au logement, aux retraites, au marché du travail, aux finances publiques et à d'autres types de risques qui transformeront l'économie telle que nous la connaissons aujourd'hui

C'est la raison pour laquelle les organisations qui échouent à tenir compte de cette réalité vont au-devant de sérieux ennuis. De nos jours, les directeurs des ressources humaines ont une conscience aiguë de cette transformation et travaillent d'arrache-pied pour appréhender les attributs spécifiques de ces professionnels.

Le responsable de l'audit interne devra également insister sur d'autres aspects liés aux compétences relationnelles qui se perdent progressivement et qui ont pourtant leur importance

Le rôle du responsable de l'audit interne

Ces changements organisationnels touchent également l'audit interne et imposent à son responsable de vérifier les mesures prises par l'organisation pour adapter son image, développer de nouveaux livrables et services ciblant les jeunes générations, et intégrer un nouveau mode de communication avec ces dernières. Il doit également gérer correctement ses équipes et, comme indiqué dans l'étude intitulée *The Millennial Auditor* (source : *Wolters Kluwer*), de tirer profit de la maîtrise que ces générations ont des nouvelles technologies et des liens qu'elles nouent avec leur environnement.

Par ailleurs, il devra également insister sur d'autres aspects liés aux *soft skills* qui se perdent progressivement et qui ont pourtant leur importance, telles que les capacités à s'exprimer en entretien, à communiquer efficacement à l'écrit, et à rédiger un rapport d'audit interne. En outre, pour retenir les jeunes talents, il convient de miser sur l'optimisation de l'environnement de travail (Sujet incontournable n°5).

SUJET 7

CYBERSÉCURITÉ

La cybersécurité est l'un des risques prioritaires auxquels les organisations doivent faire face car le nombre de cyberattaques augmente jour après jour. Ces attaques sont de plus en plus sophistiquées et ont une incidence considérable sur la situation économique et sur la réputation des entreprises. Les pouvoirs publics ne sont pas à l'abri d'une telle menace. Par exemple, à eux seuls, les hackers chinois ont causé un préjudice estimé à plus de 100 millions de dollars aux réseaux de l'*US Defence Department*, selon des documents révélés par Edward Snowden.

En 2012, ce même département faisait quotidiennement l'objet de plus de 10 millions de cyberattaques. Étant donné la prolifération rapide des cybercriminels, il serait raisonnable de penser que ce chiffre a fortement augmenté depuis cette date. Autre exemple, l'*US Marine Corp*, visé par plus de 110 000 cyberattaques par heure.

Même les organisations les mieux protégées subissent des cyberattaques et sont exposées au vol de données de toutes sortes (fuites de données), qui ont des conséquences phénoménales sur leur santé économique et sur leur réputation. L'espionnage industriel fait partie des objectifs de ces cybercriminels.

Par exemple, les 20 plus grandes cyberattaques en France en 2015 ont été perpétrées dans cette optique [11] ; et en 2014, une cyberattaque contre JPMorgan Chase a compromis les comptes de 76 millions de ménages et de 7 millions de petites entreprises. Les résultats définitifs de cette attaque surpassaient de très loin les premières estimations faites par la banque et ont fait de cette opération l'une des intrusions les plus massives jamais menées.

Le 6 juillet 2016, le Parlement européen a approuvé la première Directive européenne sur la cybersécurité – la Directive sur la sécurité des réseaux et des systèmes d'information (la Directive 2016/1148 du 06 Juillet 2015 dite NIS: *Network and Information Security*)

Fruit d'une étude des menaces pesant sur l'information en Europe dévoilées entre décembre 2014 et décembre 2015, le Threat Landscape 2015 (ETL 2015) de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) propose une analyse de la situation et de la dynamique de l'environnement des cybermenaces. [12]

Protection des données : le nerf de la guerre pour les organisations

Dans ce contexte, la protection des données revêt une importance toute particulière, non seulement parce qu'il s'agit de respecter la réglementation européenne (Directive 95/46/CE et Directive 2016/680) mais également parce que l'ouverture de nouveaux canaux de communication a conduit à une hausse importante de la fraude (et notamment du risque d'usurpation d'identité).

La plupart des services bancaires ont dopé la sécurité de leurs transactions en ligne grâce aux *Two Factor Authentification Technologies (2FA),* qui consistent à vérifier l'identité à deux reprises. Ce type de solution nécessite que les utilisateurs fournissent un autre élément d'identification que le traditionnel mot de passe pour corroborer le fait qu'ils sont bien celui ou celle qu'ils prétendent être.

Le 6 juillet 2016, le Parlement européen a approuvé la première Directive européenne sur la cybersécurité – la Directive sur la sécurité des réseaux et des systèmes d'information (la Directive 2016/1148 du 06 Juillet 2015 dite NIS : *Network and Information Security*) – afin que les entreprises qui fournissent des services essentiels renforcent leurs capacités de défense contre les cyberattaques et déclarent les incidents aux autorités nationales.

Les retours d'expérience n'ont pas cessé depuis que MyDoom (le virus le plus coûteux de l'histoire de la cybersécurité, responsable d'un préjudice financier estimé à 38,5 millions de dollars) a été découvert pour la première fois en 2004 et qu'il est devenu le virus le plus rapidement propagé par mail jamais connu. Cet incident a fait prendre conscience aux organisations de l'importance de posséder des logiciels de protection modernes sur tous leurs appareils.

Mais l'anti-virus ne suffit pas. Il ne faut pas oublier que les cybercriminels utilisent également de nombreuses autres techniques, telles que l'ingénierie sociale et le hameçonnage *(phishing)*.

Dans le contexte de la sécurité de l'information, l'ingénierie sociale désigne la manipulation psychologique de personnes pour les amener à effectuer certaines actions ou à révéler des informations confidentielles. Il s'agit d'un type d'escroquerie visant à récolter des informations, à commettre une fraude ou à accéder à un système à l'aide de techniques comme le détournement de la mention « J'aime » *(like-jacking),* le piratage de liens, le hameçonnage, les *spams,* etc.

Par exemple, un vaste réseau cybercriminel international basé en Europe de l'Est est parvenu à voler un milliard de dollars en deux ans à une centaine de banques différentes dans 30 pays en ciblant les collaborateurs de ces établissements avec des courriels de hameçonnage.[13]

Le facteur humain est le maillon faible de la cybersécurité, ce qui explique pourquoi la

manipulation psychologique est si répandue parmi les victimes de cyberattaques.

Les utilisateurs qui passent une part importante de leur temps sur les réseaux sociaux sont fortement susceptibles de cliquer sur des liens publiés par des amis de confiance, que les pirates de l'information utilisent ensuite à leur profit.

Et il ne s'agit là que de quelques-unes des cyberattaques les plus fréquentes perpétrées sur les réseaux sociaux.

Renforcer la formation aux outils informatiques : une priorité pour les responsables d'audit interne

Les organisations sont déjà pleinement sensibilisées à la cybersécurité et cet aspect devrait donc constituer un pan important d'un plan d'audit interne. L'évaluation de l'efficacité des mesures de cybersécurité nécessite des experts et il incombe donc au responsable de l'audit interne de s'assurer qu'il dispose de ces compétences. Une partie de ces contrôles est souvent externalisée pour des raisons de complexité ou d'actualité.

Le responsable de l'audit interne devrait régulièrement évaluer les politiques de l'entreprise relatives à la sécurité des systèmes d'information et leur robustesse, ainsi que le degré de sensibilisation du personnel.

Tous les collaborateurs de l'organisation doivent être formés mais un accent tout particulier devrait être mis sur les cadres, compte tenu de la sensibilité des données auxquelles ils ont accès.

La cybersécurité devrait faire partie du quotidien des collaborateurs (sécurisation de la connexion Internet à la maison, cryptage des clés USB, utilisation de programmes anti-virus, téléchargement de fichiers et consultation de certaines pages, entre autres) afin d'éviter les logiciels malveillants.

La Norme 1210.A3 indique que les auditeurs internes doivent posséder une connaissance suffisante des principaux risques et contrôles relatifs aux systèmes d'information, et des techniques d'audit informatisées susceptibles d'être mises en œuvre dans le cadre des travaux qui leur sont confiés. Toutefois, tous les auditeurs internes ne sont pas censés posséder l'expertise d'un auditeur dont la responsabilité première est l'audit informatique.

Le responsable de l'audit interne devrait être informé des développements logiciels internes. Il devrait avoir l'assurance que ces développements s'accompagnent de mesures de sécurité adéquates avant que les logiciels ne soient mis en production. Des audits en continu peuvent être envisagés dans la mesure où ces systèmes évoluent sans cesse.

À cet égard, le document intitulé *Cybersecurity, a Global Challenge,* de la Bankinter Innovation Foundation, précise que des indicateurs sont nécessaires pour identifier la nocivité réelle d'un logiciel particulier, ainsi que le niveau de sécurité qu'il offre. Cependant, il est difficile de tracer la limite entre ce qui est sécurisé et ce qui ne l'est pas dans le domaine logiciel.

Le responsable de l'audit interne devrait également évaluer les protocoles d'action en cas d'attaque pour s'assurer qu'ils restent

Tous les collaborateurs de l'organisation doivent être formés mais un accent tout particulier devrait être mis sur les cadres, compte tenu de la sensibilité des données auxquelles ils ont accès

Tous les risques en matière de cybersécurité n'émanent pas obligatoirement de la toile. Ils nécessitent donc des mesures de sécurité physiques auxquelles les auditeurs internes devraient également être sensibilisés, telles que la protection des accès aux locaux ou à d'autres zones sensibles

à jour et préserver la résilience de la société (c'est-à-dire sa capacité à absorber divers chocs internes et externes et à s reprendre un fonctionnement normal).

En 2014, le *National Institute of Standards and Technology (NIST)* a établi un référentiel de contrôle qui pourrait se révéler extrêmement utile pour affronter ces risques, bien que des évaluations supplémentaires puissent être requises selon ISO 27001 et 27002 afin d'afficher des garanties plus élevées. Ce référentiel expose une série de bonnes pratiques, propose une méthode de protection de la vie privée, et formule des recommandations sur les risques et les activités de cybersécurité.

Le GTAG publié par l'IIA, *Évaluer le risque de cybersécurité – Le rôle des trois lignes de maîtrise,* explique aux auditeurs internes comment mettre à jour leurs pratiques. Le responsable de l'audit interne y trouvera une approche simple pour évaluer les risques de cybersécurité et les capacités de réponse du management, en se concentrant notamment sur la diminution du temps de réponse. [14]

Néanmoins, tous les risques de cybersécurité n'émanent pas obligatoirement de la toile. Ils nécessitent donc des mesures de sécurité physiques auxquelles les auditeurs internes devraient également être sensibilisés, telles que la protection des accès aux locaux ou à d'autres zones sensibles.

Les prestations externalisées ne doivent pas faire exception à la règle. Les prestataires qui ont accès à certaines des informations de la société devraient avoir des niveaux de sécurité similaires ou plus élevés et notre rôle est de contrôler leur activité.

SUJET 8

FRAUDE ET CORRUPTION

La fraude reste l'une des principales préoccupations de l'auditeur interne car elle affecte les organisations de toutes tailles, avec des répercussions directes sur leurs résultats financiers et leur culture d'entreprise.

Selon l'enquête 2015 *Kroll Global Fraud* menée par Kroll, société de conseil spécialisée dans la gestion de l'information et de l'intelligence économique, auprès de 768 cadres de divers secteurs dans le monde entier, 75 % des sociétés interrogées déclarent avoir été victimes d'une fraude au cours des 12 derniers mois. En outre, 81 % d'entre elles avouent que des facteurs internes sont à l'origine de la fraude.

La fraude technologique est celle qui a connu la croissance la plus rapide ces dernières années, affichant un degré de sophistication toujours plus élevé. D'après la *2016 Global Fraud Study* de l'ACFE, une organisation type perd en moyenne 5 % de son chiffre d'affaires annuel à cause de la fraude.

LA FRAUDE PROVOQUE ÉGALEMENT une perte de confiance de la part des clients. Or, les conséquences indirectes d'une dégradation de l'image de l'organisation sont difficiles à quantifier.

Cette pression s'ajoute à celle exercée par les régulateurs, d'où la nécessité d'un système de protection efficace pour éviter les sanctions administratives, voire pénales.

Les régulateurs s'assurent que les organisations ont des dispositifs de maîtrise de la corruption, du blanchiment de capitaux et de la fraude comptable, mais ces systèmes ne sont pas infaillibles. Dans 40,7 % des cas, l'organisation victime a décidé de ne pas porter plainte pour fraude, avant tout par crainte d'une mauvaise publicité (source : ACFE).

Quel que soit le contexte, il est important de déterminer comment le management s'efforce d'instaurer un environnement dans lequel les gens se comportent de façon éthique et responsable.

Au sommet de l'organisation, le responsable de l'audit interne devrait se concentrer sur l'identification des problèmes de corruption (ISO 37001) qui représentent un risque majeur pour l'organisation

Le responsable de l'audit interne devrait s'assurer que ces dispositifs de contrôle interne sont adéquats et évaluer les faiblesses qui pourraient donner lieu à une fraude. Dans ce cas, il ne devrait pas se contenter de renforcer les contrôles mais proposer de modifier les processus pour éviter qu'une telle fraude ne se produise.

Au sommet de l'organisation, le responsable de l'audit interne devrait se concentrer sur l'identification des problèmes de corruption (ISO 37001) qui représent un risque majeur pour l'organisation, et, dans d'autres secteurs de la structure organisationnelle, mettre l'accent sur le détournement d'actifs, dont l'impact est généralement moindre.

Il ne fait aucun doute que les organisations devraient continuer d'investir dans des programmes de détection permettant l'identification des indicateurs de risques les plus courants et de renforcer les programmes de prévention, car c'est le meilleur gage d'efficacité.

Le développement d'un programme de lutte contre la fraude et l'instauration d'une culture éthique au sein de l'organisation et vis-à-vis des tiers en lien avec l'activité de la société constituent les meilleurs facteurs de dissuasion.

Ce programme devrait fixer une tolérance zéro envers tous les types de comportements frauduleux, quels que soient les montants concernés et le niveau de l'organisation touché.

Mais comment peut-on détecter la fraude ? Il convient d'admettre que dans la plupart des cas, la fraude est révélée par chance ou fait l'objet d'une dénonciation. La chose inquiétante (qui porte atteinte à la réputation de notre profession) est que, souvent, un laps de temps considérable s'écoule sans qu'aucune activité de contrôle ou de supervision n'ait détecté le problème.

La première action qu'un responsable de l'audit interne devrait prendre est d'analyser le dispositif d'alerte, un outil essentiel qui devrait être renforcé.

Pour que cet outil soit efficace, il doit pouvoir offrir une réponse instantanée au lanceur d'alerte, tout en garantissant sa protection ainsi que des mesures fermes dans les cas où les faits sont avérés.

Les collaborateurs n'utiliseront ce moyen de communication que s'ils peuvent s'y fier entièrement et voient que le dispositif fonctionne sans que le lanceur d'alerte ne subisse de représailles. En outre, cet outil permet de détecter les problèmes de contrôle interne susceptibles d'affecter le plan de prévention des risques criminels, en proposant une solution immédiate au problème et en révisant le plan concerné.

Les tâches liées à la fraude nécessitent des compétences très spécifiques de la part de l'auditeur interne, et une formation continue sur les types de fraude existants et les techniques de détection correspondantes devraient être une priorité pour n'importe quel service d'audit interne. Les auditeurs internes n'ont pas besoin d'être experts en matière de fraude, mais comme indiqué dans la Norme 1210.A2, ils doivent posséder des connaissances suffisantes pour évaluer le risque de fraude et la façon dont ce risque est géré par l'organisation.

En septembre 2016, le COSO a publié un *Guide de gestion du risque de fraude* aligné et cohérent avec le Référentiel 2013, qui a pour vocation d'offrir aux organisations des recommandations de bonnes pratiques d'évaluation du risque de fraude. [15]

Dans ce type de mission, il convient de partir du principe que tous les éléments probants récoltés sont susceptibles d'être utilisés au tribunal et que nous devons par conséquent agir avec toute la conscience

professionnelle nécessaire pour ne pas invalider une preuve potentielle.

Les systèmes d'information des organisations sont d'excellents outils de détection de la fraude. L'audit interne devrait exploiter le potentiel du *big data* pour identifier les schémas récurrents et les comportements inhabituels, et enquêter plus avant. Depuis plus de dix ans, l'intelligence artificielle facilite ces analyses et les améliore constamment. Elle est utilisée par des praticiens avant-gardistes pour prévenir la fraude dans des secteurs tels que les télécommunications, l'assurance et la banque.

Il existe plusieurs façons de lutter contre la fraude grâce à l'intelligence artificielle, telles que les réseaux neuronaux libres ou supervisés, particulièrement utilisés dans l'univers de la finance pour éviter les « fraudes au Président » ainsi que les escroqueries à la carte de crédit ou de débit.

Les modèles de Markov cachés ou les réseaux bayésiens sont aussi couramment employés pour identifier des schémas récurrents, dans lesquels les probabilités sont définies et l'incertitude concernant le fait qu'un comportement spécifique résulte d'une fraude se trouve réduite.

La tâche serait plus simple si les schémas récurrents coïncidaient parfaitement avec les enregistrements des transactions, mais la fraude change constamment de visage, ce qui la rend difficile à détecter lorsqu'elle est commise pour la première fois.

L'avantage des réseaux bayésiens est qu'ils bénéficient d'une période d'apprentissage beaucoup plus courte que les réseaux neuronaux, mais les réseaux neuronaux, eux, jaugent les nouveaux exemples plus rapidement. Le document : *Credit Card Fraud Detection Using Advanced Combination Heuristic and Bayes' Theorem* [16] en donne un bon exemple.

Pour l'heure, la meilleure manière de lutter contre la fraude est d'utiliser un concept relativement nouveau, l'« intelligence augmentée ». L'essence de l'intelligence augmentée est de combiner les aptitudes humaines les plus poussées et les meilleurs avantages des machines. [17]

Aujourd'hui, les techniques de détection de la fraude continuent de progresser et le ratio coût/bénéfice ne cesse de diminuer en raison d'un nombre plus faible de faux positifs (source : *Data Mining Techniques in Fraud Detection*). [18]

En 2014, Canal de Isabel II Gestión, la plus grande régie de la Ville de Madrid, chargée de la gestion du cycle de l'eau dans toute la région madrilène, a décidé d'acheter des images haute définition au CNES, l'agence spatiale française dont les satellites Pléaides sont capables de prendre des photos de n'importe quel endroit du globe à une résolution extrêmement élevée.

Après avoir passé au crible 120 000 piscines et 23 000 hectares de parcs, prairies et jardins, le service Recherche, développement et innovation de Canal de Isabel II a mis au jour un « écart » de 10 % dans la consommation d'eau. Cet écart a été analysé par la division Fraude pour déterminer les responsabilités.

Le management devrait prendre conscience que davantage de contrôles impliquent moins de fraude. La gestion intégrée *(Integrated Thinking)* et la supervision de la culture d'entreprise (sujet incontournable n°3) sont également des facteurs de dissuasion essentiels dont le responsable de l'audit interne devrait soutenir le développement.

Les auditeurs internes n'ont pas besoin d'être experts en matière de fraude, mais comme indiqué dans la Norme 1210.A2, ils doivent posséder une connaissance suffisante

SUJET 9

CONSEILLER DE CONFIANCE

La confiance est essentielle pour que l'ensemble d'une organisation fonctionne correctement. Le rapport *Global Generations 3.0*, publié par EY en juin dernier, au terme d'une enquête conduite auprès de quelque 10 000 actifs entre 19 et 68 ans dans 8 pays, montre qu'à peine 46 % des collaborateurs ont « une grande confiance » dans leur employeur, et que seuls 49 % ont « une grande confiance » dans leur responsable ou dans leurs collègues.

Ces chiffres font apparaître un risque qui doit être maîtrisé car il met l'environnement de travail (sujet incontournable n°5) à rude épreuve, conduisant à une augmentation du taux de rotation du personnel et à une prise de décision bancale.

Progressivement, le management devrait instaurer des leviers de confiance tels que la transparence, la sincérité, la capacité à admettre ses erreurs, et, bien entendu, véhiculer les valeurs de l'entreprise à travers ses actes et pas seulement à travers ses paroles.

Cependant, en retour, à qui la direction générale peut-elle faire confiance ? À qui doit-elle faire appel pour des conseils sur les décisions importantes ?

Le rôle de l'auditeur interne comme conseiller de confiance

Il est important que le responsable de l'audit interne valorise son poste au sein de l'organisation en devenant ce conseiller de confiance, car à défaut, il risque de passer à côté de la stratégie adoptée et de perdre

de l'emprise sur les décisions. Il deviendrait alors un personnage sans envergure qui ne pourrait agir qu'a posteriori, une fois que le mal a été fait.

Le responsable de l'audit interne devrait adopter une attitude proactive dans ce domaine car il possède toutes les compétences pour mener cette tâche à bien. Cependant, il doit au préalable avoir surmonté certains obstacles liés à la culture d'entreprise.

En premier lieu, il doit gagner la confiance du management en démontrant que l'audit interne n'est pas qu'un simple fournisseur d'assurance mais qu'il peut aussi apporter d'autres services à forte valeur ajoutée. Si besoin, le responsable de l'audit interne devrait sensibiliser le reste de l'organisation à son action via une campagne de sensibilisation interne.

En deuxième lieu, il devrait gagner la confiance du management en associant les dirigeants à l'élaboration du plan d'audit annuel, en leur fournissant des informations et en prenant en compte leurs demandes ; autrement dit, en reconnaissant leur place dans l'environnement de contrôle.

Il est également essentiel que le responsable de l'audit interne bénéficie d'un appui suffisant pour entreprendre cette démarche. Le comité d'audit devrait soutenir le responsable de l'audit interne. Il aura un rôle décisif dans les relations qu'entretient le responsable de l'audit interne avec les dirigeants de l'organisation.

Le comité d'audit devrait demander au responsable de l'audit interne, au moins une fois par an, les actions entreprises dans ce domaine. Le but principal d'un conseiller de confiance au sein de l'organisation est de contribuer à l'efficacité des prises de décisions.

Ce statut dépendra du positionnement du responsable de l'audit interne. Par exemple, le fait qu'il siège au comité exécutif et qu'il facilite la compréhension du plan stratégique de l'organisation et du développement de l'activité.

Les connaissances, l'utilisation des technologies et la bonne qualité des données, garante d'une information fiable sont autant d'atouts pour améliorer la prise de décision.

Chaque fois que le management aborde un sujet, il est important qu'il dispose d'informations fiables et exhaustives. Cependant, la difficulté provient du fait que les décisions doivent souvent être prises dans un laps de temps très court. Un tel processus implique de soupeser les différentes options ainsi que les objectifs recherchés et d'analyser en détail les conséquences susceptibles d'affecter l'activité et la structure d'assurance de l'organisation.

Le responsable de l'audit interne veillera à ce qu'aucune action prise par le management n'affaiblisse la structure de contrôle interne. La prise de décision n'étant pas un processus purement rationnel, il devra faire preuve de jugement. Il présentera des conclusions compréhensibles, s'adaptera à chaque partie prenante et fera preuve d'une bonne dose d'intelligence émotionnelle.

Il ou elle devrait avoir le courage et l'assurance nécessaire pour donner des avis que d'autres n'oseraient pas formuler, et surtout, ne pas craindre de déplaire au management.

La position qu'occupe l'audit interne dans l'organisation constitue un avantage car elle

Le responsable de l'audit interne veillera à ce qu'aucune action prise par le management n'affaiblisse la structure de contrôle interne

confère au responsable de l'audit interne l'indépendance requise pour déclencher la mise en œuvre de toutes sortes d'évaluations sans se sentir conditionné par l'environnement ou la connaissance de la structure organisationnelle, le statut du contrôle interne et les risques qui lui permettent de bénéficier d'une vue d'ensemble que d'autres n'ont pas.

L'un des principaux attributs d'un conseiller de confiance est d'être un excellent communicant capable d'écouter et d'analyser l'information d'un œil critique, objectif et rationnel, sans interférences

La situation dépeinte dans le conte pour enfants *Les Habits neufs de l'empereur* se retrouve dans la structure de nombreuses sociétés : aveuglé par les gesticulations d'un escroc et le silence de sa cour, qui n'osait le contredire, l'empereur défila nu devant ses sujets en croyant qu'il était paré d'un vêtement somptueux. Ses conseillers voulaient éviter tout conflit et confirmaient les propos de l'empereur, sans chercher à argumenter.

L'un des principaux attributs d'un conseiller de confiance est d'être un excellent communicant capable d'écouter et d'analyser l'information d'un œil critique, objectif et rationnel, sans interférences.

Le responsable de l'audit interne devrait tenir compte d'infimes détails susceptibles de passer inaperçus, sans pour autant perdre de vue le tableau d'ensemble. Lors de la formulation de recommandations, ces éléments peuvent se révéler utiles pour gagner la confiance du management.

Il se peut que le bénéficiaire désapprouve d'emblée certaines recommandations, et c'est pourquoi le responsable de l'audit interne devrait être capable de persuader son auditoire des avantages qu'il peut y avoir à mettre en place un plan d'action donné. Le bénéficiaire ne doit pas percevoir ces recommandations comme un ordre ou une contrainte mais plutôt comme un avis constructif qui incorpore des suggestions inspirées de bonnes pratiques. La connaissance des bonnes pratiques est un facteur de différenciation qui sera valorisé par l'organisation.

L'organisation ne se contente plus de faire les choses bien mais aspire plutôt à les faire mieux que quiconque, et, dans un environnement aussi volatile et complexe, l'avis d'un conseiller de confiance peut lui donner une longueur d'avance sur ses concurrents.

Les responsables de l'audit interne sont formés à ce rôle difficile de conseiller de confiance mais ils ne devraient pas oublier qu'ils sont régis par les normes d'audit interne établies par le Cadre de Référence International des Pratiques Professionnelles de l'Audit Interne (CRIPP). Ils devraient donc faire preuve de la plus grande conscience professionnelle afin de ne pas franchir certaines lignes rouges connues de tous et qui font l'objet de diverses publications des instituts l'IIA.

SUJET 10

TRANSFORMATION

Non seulement la révolution technologique transforme les organisations et les rend plus efficientes, mais elle provoque aussi des changements radicaux dans presque tous leurs processus, notamment les processus relatifs aux relations avec les clients, les fournisseurs, voire les collaborateurs.
Ces nouveaux processus représentent un changement culturel certain : la digitalisation des opérations, l'automatisation des processus et l'autogestion des clients dégagent d'énormes bénéfices. Désormais, les logiciels intuitifs occupent une grande place et, souvent, prennent en charge la quasi-totalité des activités opérationnelles tout en réduisant le nombre d'erreurs de traitement. La fraude liée aux systèmes d'information est celle qui a connu la croissance la plus rapide ces dernières années, affichant un degré de sophistication toujours plus élevé.

CETTE NOUVELLE MANIÈRE DE FAIRE DES AFFAIRES transforme en profondeur les processus, modifie l'exposition aux risques et provoque une révolution interne sans précédent.

Toutefois, le progrès technologique n'est pas le seul facteur de bouleversement des organisations. D'autres changements sont imputables à la clientèle, dans la mesure où les organisations tentent de s'adapter aux comportements d'une nouvelle génération de clients, et de se conformer dans le même temps aux exigences réglementaires accrues en termes de protection de la vie privée.

Le client n'est plus un sujet passif destinataire d'un produit ou d'un service, mais plutôt un employé du service marketing, grâce aux réseaux sociaux, ou encore un gestionnaire des données chargé de saisir, de corriger et de modifier les informations qui lui sont propres. On peut dire que les clients font désormais partie intégrante des processus de l'organisation.

Les risques tendent à augmenter tout au long de cette période d'adaptation et, de surcroît, les modifications qui surviennent ont pour effet de fragiliser le système de contrôle interne.

Les risques tendent à augmenter tout au long de cette période d'adaptation et, de surcroît, les modifications qui surviennent ont pour effet de fragiliser le système de contrôle interne

Il est essentiel que le responsable de l'audit soit pleinement conscient de la transformation susceptible d'avoir lieu, car cela signifie que la société peut se retrouver exposée à de nouveaux risques et qu'une révision constante du système de contrôle interne en vigueur dans l'organisation s'impose (ce qui fonctionne aujourd'hui peut ne pas fonctionner demain).

À mesure que l'organisation évolue, l'audit interne change également ; et pas uniquement à cause des transformations technologiques.

Le rôle de l'audit interne s'est renforcé ces dernières années car les parties prenantes en ont fait le pourvoyeur d'une assurance raisonnable sur le fonctionnement de l'organisation.

L'identification claire et nette de cette responsabilité est source de satisfaction et montre la profession sous son meilleur jour. Toutefois, là encore, l'excellence est de mise, ce qui signifie que cette transformation sera observée en tenant compte de divers facteurs.

Le responsable de l'audit interne devrait utiliser son expérience et sa méthode pour évaluer la conception de ces processus apparemment « parfaits » et détecter à temps les faiblesses du contrôle interne afin qu'elles puissent être corrigées.

Il devrait également évaluer les risques significatifs auxquels l'organisation est exposée, en mettant l'accent sur les risques liés à la gouvernance (sujet incontournable n°2), sans oublier ceux liés aux tiers.

L'audit interne devrait donc avoir une approche à la fois descendante *(top to bottom)* et transversale *(inside to out),* en accordant l'importance nécessaire à chaque activité.

Le périmètre d'audit ne cesse de s'élargir, ce qui crée des problèmes non seulement lors de l'élaboration du plan d'audit interne mais également pour sa bonne mise en œuvre.

On demande aux services d'audit interne d'exploiter cet environnement technologique pour passer en revue, presque en temps réel, toutes les données en lien avec un processus et identifier tout comportement anormal révélateur d'une fraude ou d'une faille de la sécurité de l'information, ou susceptible de perturber l'activité.

Il ne serait pas très logique que l'ensemble de l'organisation fasse sa révolution numérique et que le service d'audit interne se prive des logiciels qui lui permettraient de réduire, voire de supprimer toute opération manuelle.

L'audit interne doit se montrer proactif, s'intéresser à la gestion prédictive, et cette transformation devrait être mise en œuvre pour diriger l'attention non plus sur les processus, mais plutôt sur les aspects stratégiques les plus décisifs pour la continuité de l'activité.

Pour des questions d'efficience, l'audit interne devrait abandonner les procédures administratives particulièrement archaïques qui génèrent une consommation excessive de ressources et revoir ses méthodes.

De nombreuses entreprises exigent de faire davantage avec moins de ressources : les auditeurs internes peuvent également y parvenir en réorientant les missions, en explicitant la source d'une recommandation et en optimisant le recours aux systèmes d'information.

Selon le rapport du CBOK intitulé *Étude comparative de la maturité de l'audit interne*, l'utilisation des systèmes d'information est un indicateur de la maturité du service d'audit interne.

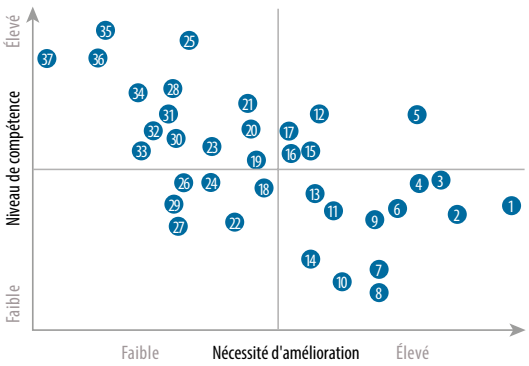
Parmi les responsables de l'audit interne interrogés, 39 % déclarent que leur département s'appuie sur des systèmes d'information appropriés, ou utilise de manière généralisée les systèmes d'information d'un bout à l'autre du processus d'audit, y compris l'extraction et l'analyse de données.

Le comité d'audit devrait également être conscient que ce nouvel environnement technologique nécessite un budget accru en raison des investissements en matière d'équipements et de logiciels informatiques, et des ressources dédiées à la formation.

En outre, les équipes d'audit auront besoin de nouvelles compétences, devront afficher une plus grande pluridisciplinarité et nécessiteront plusieurs responsables dotés d'une grande expertise.

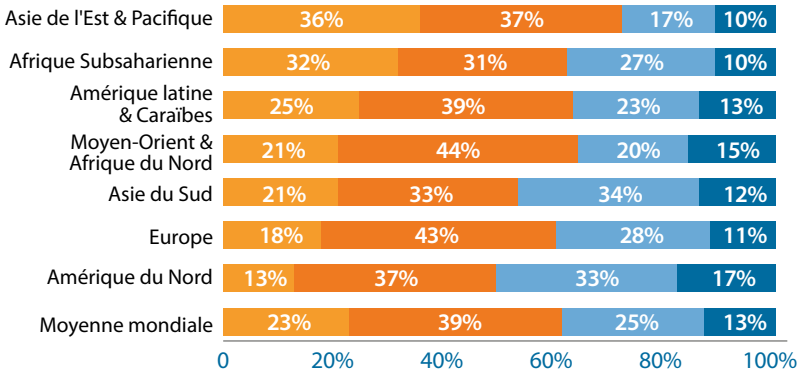
Selon la publication de Protiviti intitulée *Arriving at Internal Audit's Tipping Point. Amid Business Transformation 2016* [19], la connaissance du déroulement actuel de l'audit peut être schématisée comme suit :

Connaissance du déroulement de l'audit – Carte perceptuelle



Source : Protiviti

Utilisation de systèmes d'information en appui des processus d'audit interne par région



Utilisation de systèmes et de processus essentiellement manuels

Utilisation de documents de travail électroniques ou autres outils bureautiques liés aux systèmes d'information

Méthodologie d'audit soutenue par des systèmes d'information

Utilisation généralisée de systèmes d'information d'un bout à l'autre du processus d'audit, y compris l'extraction et l'analyse de données

Source : CBOK 2015

Numéro	Connaissance du déroulement de l'audit	Numéro	Connaissance du déroulement de l'audit
1	Outils d'analyse des données – Analyse statistique	20	Audit en continu
2	Audit des systèmes d'information – Sécurité	21	Audit opérationnel –fondée sur une approche par les risques
3	Audit des systèmes d'information – Continuité	22	Audit des systèmes d'information – Opérations informatiques
4	Fraude – Détection/investigation de la fraude	23	Évaluation du risque – Processus, emplacement, niveau transactionnel
5	Programme d'assurance et d'amélioration qualité (Norme 1300 de l'IIA) – Revues continues (Norme 1311 de l'IIA)	24	Audit des systèmes d'information – Contrôle du changement
6	Audit des systèmes d'information – Développement de programme	25	Planification de l'audit – Processus, emplacement, niveau transactionnel
7	Évaluation du risque – Enjeux émergents	26	Fraude – Évaluation du risque de fraude
8	Audit des systèmes d'information – Nouvelles technologies	27	Audit des systèmes d'information – Gouvernance des SI
9	Faire connaître l'audit interne en interne	28	Audit opérationnel – Efficacité des coûts / réduction des coûts
10	Techniques d'audit assistées par ordinateur (CAAT)	29	Programme d'assurance et d'amélioration qualité (Norme 1300 de l'IIA) – Revues périodiques (Norme 1311 de l'IIA)
11	Pilotage continu	30	Fraude – Risque de fraude
12	Outils d'analyse des données – Échantillonnage	31	Approche descendante fondée sur les risques pour évaluer le contrôle interne relatif au reporting financier
13	Fraude – Gestion/prévention	32	Évaluation du risque – À l'échelle de l'entité
14	Outils d'analyse des données – Manipulation des données	33	Techniques d'auto-évaluation
15	Audit opérationnel – Efficacité, efficience et économie de l'approche opérationnelle	34	Présentation à la direction générale
16	Programme d'assurance et d'amélioration qualité (Norme 1300 de l'IIA) – Évaluation externe (Norme 1312 de l'IIA)	35	Planification de l'audit – À l'échelle de l'entité
17	Fraude – Pilotage	36	Rédaction de rapports
18	Gestion des risques de l'entreprise	37	Principes d'échantillonnage en audit
19	Fraude – Audit		

L'audit interne devrait donc avoir une approche à la fois descendante *(top-down)* et tranversale *(inside-outside)*, en accordant l'importance nécessaire à chaque activité

On observe qu'en termes de formation, un écart important subsiste entre le niveau de compétence d'où la nécessité d'améliorations substantielles.

Un facteur primordial de la transformation du service et de l'accroissement de son niveau de maturité réside dans l'amélioration de l'utilisation des données via des missions continues.

Le recours aux données pour les audits en continu est essentiel et ce type d'approche devient de plus en plus incontournable.

Outre la maîtrise des frais de déplacement, l'audit en continu permet d'identifier plus rapidement les incidents et de déclencher des mesures correctives appropriées.

L'automatisation d'une grande partie du processus signifie que les auditeurs internes peuvent se focaliser sur l'analyse des signaux d'alerte.

Indépendamment des changements qui interviennent dans les processus de l'audit interne, l'accroissement des différents prestataires d'assurance est aussi fulgurante. En outre, leurs responsabilités deviennent si complexes et transversales qu'une coordination devient nécessaire pour éviter les inefficacités et les lacunes en matière d'assurance.

Une cartographie des prestataires d'assurance semble alors particulièrement adapté et souligne l'importance de l'audit interne dans le bon fonctionnement des dispositifs de contrôle des risques au sein de l'organisation.

Le responsable de l'audit interne ne devra non seulement s'efforcer de superviser le fonctionnement adéquat de la structure dans son ensemble, ce qui lui vaudra la confiance du comité d'audit, mais il devra également veiller à l'efficience du fonctionnement, source de reconnaissance de la part de la direction générale.

SOURCES

1 https://openknowledge.worldbank.org/bitstream/handle/10986/24319/9781464807770.pdf?sequence=6

2 http://www.realinstitutoelcano.org/wps/portal/web/rielcano_en/publication?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/publications/elcano-global-presence-report-2016

3 https://www.aqmen.ac.uk/sites/default/files/TheViewFromTheContinent_REPORT.pdf

4 Baisse du tourisme en région parisienne #AFP pic.twitter.com/fzbzXz9EIJ— Agence France-Presse (@afpfr) 23 August 2016.

5 https://europa.eu/globalstrategy/sites/globalstrategy/files/about/eugs_review_web_6.pdf

5.1 http://www.ibe.org.uk/list-of-publications/67/47

6 Cadres : quels ont été les métiers les plus porteurs en 2016 ? / Le Monde, 13 septembre 2016

7 http://www.dfs.ny.gov/about/ea/ea160819.pdf

8 https://www.fca.org.uk/news/press-releases/fca-introduces-new-rules-whistleblowing

9 Source : McCann Truth Central 2016

10 Source : United Nations

11 http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/la-france-a-ete-la-cible-d-une-vingtaine-de-cyberattaques-majeures-en-2015-598189.html

12 https://www.enisa.europa.eu/publications/etl2015

13 Kaspersky

14 https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Assessing-Cybersecurity-Risk-Roles-of-the-Three-Lines-of-Defense.aspx

15 http://www.coso.org/documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf?_ga=1.192669539.870338647.1474276086

16 http://www.ijircce.com/upload/2015/april/13_Credit.pdf

17 http://jolt.richmond.edu/v17i3/article11.pdf

18 http://ojs.jdfsl.org/index.php/jdfsl/article/viewFile/180/108

19 https://www.protiviti.com/sites/default/files/united_states/insights/2016-internal-audit-capabilities-and-needs-survey-protiviti.pdf