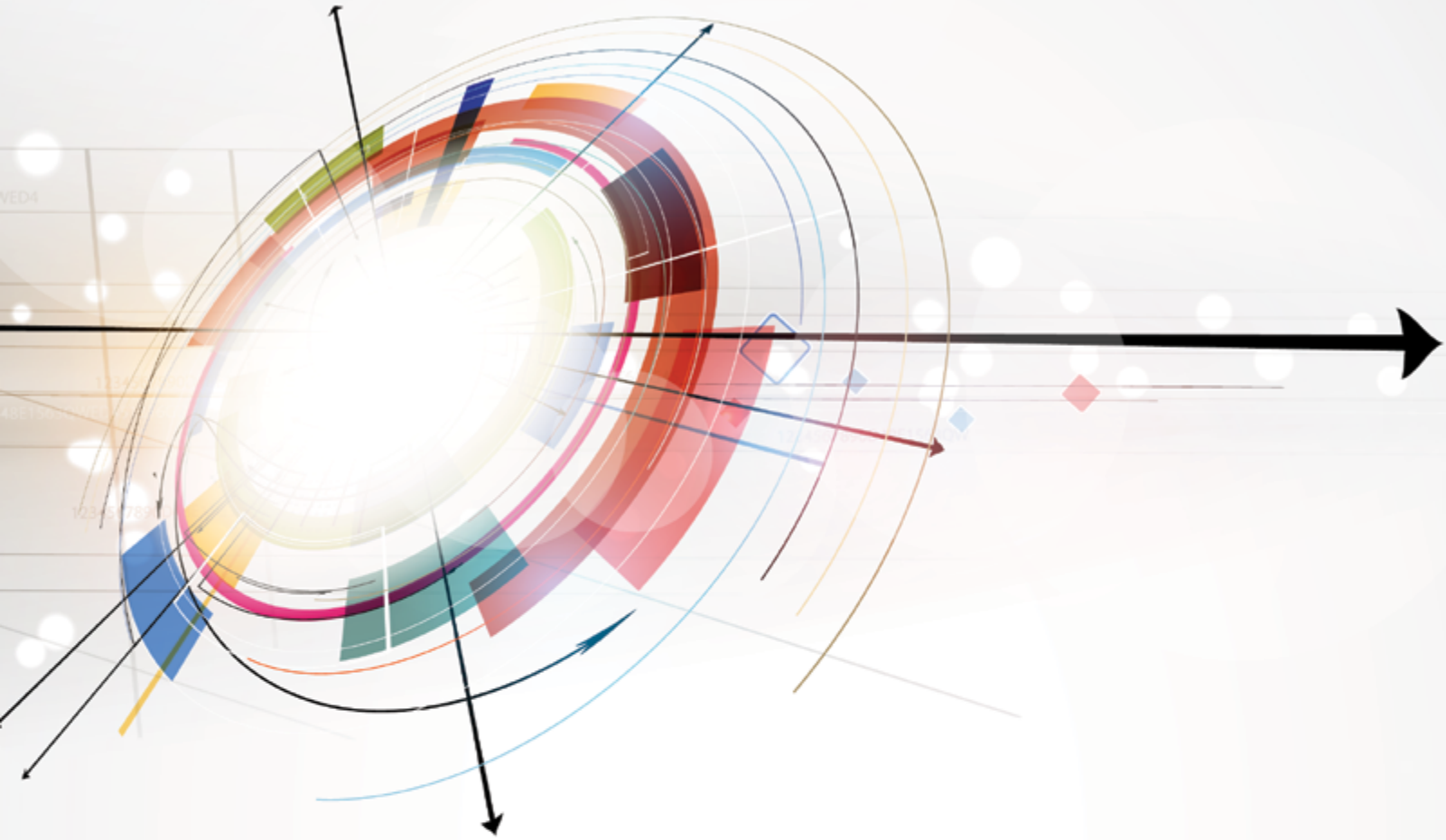

PERSPECTIVES INTERNATIONALES

2018 : Principaux risques auxquels sont confrontés les responsables de l'audit interne

The Institute of Internal Auditors

Numéros précédents

Pour accéder aux numéros précédents de Global Perspectives and Insights, visitez le site à l'adresse suivante www.theiia.org/gpi.

Commentaires des lecteurs

N'hésitez pas à nous faire parvenir vos questions et vos commentaires à l'adresse suivante : globalperspectives@theiia.org

Table des matières

Introduction

2018 : nouvelle année, nouvelles lois, réglementations, opinions, idées, technologies, et nouveaux risques. L'environnement économique actuel est sensiblement différent de ce qu'il était autrefois. Il est plus complexe et plus connecté. Les organisations sont confrontées à de nouveaux risques inconnus, mais aussi à des opportunités inexploitées. Au vu des nouvelles opportunités et des défis et risques potentiels à venir, qu'ils soient attendus ou spécifiques à 2018, les plans d'audit devraient être considérés comme des cadres modulables en fonction des événements, et notamment des perturbations.

Grâce à sa vision globale de l'organisation, l'audit interne aide cette dernière à atteindre ses objectifs en proposant une approche disciplinée et systématique pour évaluer et améliorer l'efficacité des processus de management des risques, de contrôle et de gouvernance. Les régulateurs et les comités d'audit veulent l'assurance que les dispositifs de management des risques sont adéquats pour répondre aux menaces liées à la forte concurrence, au développement des technologies ou encore à l'évolution des tendances du marché et des réglementations (cf. Internal Audit Future Trends: Emerging Trends and High-impact Areas of Focus).

Alors qu'on attend d'eux qu'ils apportent plus de valeur ajoutée et un soutien plus stratégique à tous les secteurs d'activité, les auditeurs doivent s'assurer que leurs travaux tiennent compte de tous les risques importants, particulièrement les risques stratégiques et opérationnels. L'audit interne doit être réactif et capable de s'adapter à un environnement des risques dynamique.

Les risques évoluent et même les plans d'audit les mieux conçus doivent être souples et modifiables à mesure que de nouveaux risques émergent à tous les niveaux de l'organisation. Ce document traite des cinq principaux risques (pour l'audit interne ou l'organisation) auxquels sont confrontés les responsables de l'audit interne, selon les instituts affiliés de l'IIA. Ces risques sont : la gestion des talents, l'analyse de données, la cybersécurité, les réglementations et la réponse aux perturbations.

Gestion des talents

La gestion des talents est constamment une préoccupation majeure des responsables de l'audit interne et de leurs équipes. Au cours des dernières années, les responsables de l'audit interne se sont efforcés de trouver des candidats dotés des compétences nécessaires pour remplir de nouvelles fonctions et traiter les risques existants et inédits. De toute évidence, les personnes compétentes pour répondre aux besoins changeants de l'audit interne ne sont pas légion. À cela s'ajoute l'enjeu qui consiste à mettre en phase l'environnement de travail avec les caractéristiques uniques de la génération milléniale qui nourrit des attentes

différentes et plus élevées en matière de soutien et d'appréciation, a une vision spécifique de l'environnement de travail et préfère des horaires de travail plus flexibles (Cf. 4 Strategies for Bridging the Internal Audit Talent Gap).

En 2015, attirer et retenir des talents était une priorité élevée ou absolue pour plus de 40% des personnes ayant participé à une enquête mondiale de l'IIA, et plus de la moitié ont imputé le déficit de connaissances au nombre limité des auditeurs compétents. En 2017, en réponse à une étude de l'*IIA Audit Executive Center®* (AEC®), une grande majorité (79 %) des quelque 200 responsables de l'audit interne sondés ont identifié la gestion des talents comme un risque extrêmement/très important pour la profession d'audit interne. Selon KPMG, le talent, ou l'absence de talent, est considéré par les administrateurs comme un risque d'entreprise. Compte tenu de la mondialisation croissante des organisations, la main d'œuvre évolue en permanence, rendant la gestion des talents cruciale. La pénurie de talents à l'échelle mondiale peut avoir pour conséquence l'incapacité à retenir les compétences en matière de direction parce que, d'une part, le vivier de futurs dirigeants n'est plus aussi foisonnant et, d'autre part, les candidats sont incapables d'assumer des fonctions essentielles, remettant en cause l'atteinte des objectifs stratégiques. Les organisations se rendent compte qu'elles ne sont pas en mesure d'accompagner et de guider les nouvelles générations ou de fidéliser les meilleurs talents ou les talents spécialisés, ce qui entraîne la perte du capital intellectuel et de l'avantage concurrentiel. En outre, les retraités creusent constamment le déficit de compétences (cf. Boardroom Questions: Talent Management… or Talent Risk?).

« Si l'audit interne doit être préparé pour l'avenir, l'un des cinq impératifs qu'il doit aborder est l'agilité. Nous devons être suffisamment agiles pour identifier et traiter les risques émergents et pour évaluer les risques en continu afin d'adapter notre périmètre d'audit en conséquence. Nous devons être suffisamment agiles pour reconnaître nos lacunes et les combler rapidement. La réussite appartient aux fonctions d'audit interne qui adoptent une stratégie dynamique de gestion des talents ».

Richard Chambers,
Président et Directeur Général
de l'IIA

Pire encore, en raison des risques émergents, tels que l'analyse de données, la gestion des parties prenantes, la cybersécurité, la durabilité et les diverses incertitudes notamment politiques, les organisations attendent davantage de leurs auditeurs internes. L'époque où ces derniers ne réalisaient que des audits financiers et de conformité est révolue.

Bien qu'il ne s'occupe pas des ressources humaines, l'audit interne devrait évaluer la *manière* dont la direction générale gère les risques dans ce domaine. Les organisations d'aujourd'hui ont besoin et s'attendent à ce que les auditeurs internes adoptent une approche plus holistique de l'audit, en y incluant la surveillance des risques intégrée et la création de valeur. C'est pour cette raison que la recherche des meilleurs talents, compétences et forces pour l'audit interne est devenue très concurrentielle.

Sans les compétences adéquates, l'audit interne est susceptible d'omettre ou de ne pas auditer de manière approfondie des risques spécifiques et non traditionnels liés à la technologie, à la géopolitique, à l'économie, à l'évolution des rapports d'entreprise, à la culture et aux réglementations locales et internationales. D'après la Society for Human Resource Management, la capacité des auditeurs internes à sortir de leurs domaines de compétences traditionnels, à savoir la finance, l'opérationnel et les SI, et à examiner la situation dans son ensemble, est cruciale.

Une fonction d'audit interne qui développe ses compétences de manière réfléchie et réalise ses missions en se fondant sur une compréhension plus globale du profil de risque de l'organisation sera mieux préparée à servir cette dernière. Une partie de cette préparation consiste à attirer des personnes dotées d'un esprit critique aiguisé, d'une bonne connaissance de l'organisation et de son environnement, mais aussi d'une expertise dans des domaines spécifiques ou de connaissances sectorielles particulières. Les risques émergents non traditionnels influenceront l'univers d'audit. Par conséquent, l'audit interne doit mobiliser ses compétences, les approfondir et les élargir.

Il est impératif que les responsables de l'audit interne encouragent les auditeurs à enrichir leur expérience et leurs compétences et prennent en considération la « nouvelle réalité » des risques lors de l'évaluation et de l'exécution des plans d'audit. Mais ne vous méprenez pas, la formation traditionnelle à l'audit reste pertinente ; mais la formation et l'ouverture, l'adaptabilité, de bonnes aptitudes relationnelles et la connaissance des processus et des opérations sont essentielles pour s'orienter dans le nouveau monde des affaires.

La capacité à gérer tous les talents est indispensable au succès de l'audit interne et peut apporter des avantages à long-terme, outre le fait de combler des pénuries ponctuelles de personnel. Pour optimiser les efforts déployés en matière de gestion des talents, les responsables de l'audit interne et la direction générale devraient mettre en œuvre des approches réfléchies et bien conçues visant à restructurer et à améliorer leur main-d'œuvre. Pour être efficaces et pour créer, impliquer et conserver la meilleure fonction d'audit interne possible face aux nouveaux risques, les responsables de l'audit interne doivent élaborer des stratégies qui consistent à évaluer les attentes vis-à-vis des collaborateurs actuels et des futures recrues et, tout aussi important, identifier ce que les collaborateurs ont besoin d'apprendre de leurs responsables pour évoluer et prospérer.

Une stratégie de gestion des talents bien étudiée dépend d'une combinaison d'approches. Les responsables de l'audit interne ne seront pas en mesure de se sortir d'une pénurie de talents par le biais du recrutement. Rares sont les candidats dotés des compétences nécessaires pour faire face aux risques de demain, notamment en matière de science des données, d'esprit d'innovation, de raisonnement critique/analytique, de communication, etc. Une stratégie efficace consiste à identifier les qualités et les compétences nécessaires, et les efforts continus à entreprendre pour acquérir, développer et fidéliser les meilleurs talents.

Objectifs

- Les compétences collectives de l'audit interne sont déterminées par les risques qui définissent le périmètre d'intervention de l'audit interne.
- Les responsables de l'audit interne, le comité d'audit, et la direction générale ont une solide compréhension des compétences nécessaires pour atteindre

Point d'attention

Norme de l'IIA 1210 : Compétence

Les auditeurs internes doivent posséder les connaissances, les savoir-faire et les autres compétences nécessaires à l'exercice de leurs responsabilités individuelles.

L'équipe d'audit interne doit collectivement posséder ou acquérir les connaissances, les savoir-faire et les autres compétences nécessaires à l'exercice de ses responsabilités.

Norme de l'IIA 1230 : Formation professionnelle continue

Les auditeurs internes doivent améliorer leurs connaissances, leurs savoir-faire et autres compétences par une formation professionnelle continue.

Point d'attention

Norme de l'IIA 1220 : Conscience professionnelle

Les auditeurs internes doivent apporter à leur travail la diligence et le savoir-faire que l'on peut attendre d'un auditeur interne raisonnablement averti et compétent. La conscience professionnelle n'implique pas l'infaillibilité.

1220.A2 – Pour faire preuve de conscience professionnelle, l'auditeur interne doit envisager l'utilisation de techniques d'audit informatisées et d'analyse de données.

les objectifs de l'organisation, ainsi que du coût total des effectifs de l'audit interne.

- L'audit interne a mis en œuvre un processus de gestion de la performance cohérent.
- Les responsables de l'audit interne ont la capacité d'accompagner, de soutenir et d'attirer les nouvelles générations mais aussi des personnes issues de diverses générations qui débutent dans l'audit interne.
- Un plan de carrière formel est prévu pour chaque auditeur interne.
- L'audit interne a élaboré des programmes pour accueillir de nouvelles recrues et pour former continuellement l'ensemble des collaborateurs à la culture, à l'appétence pour le risque et à l'orientation stratégique de l'organisation.

Actions

- Examiner l'évaluation des risques ainsi que le plan d'audit et déterminer les compétences nécessaires pour exécuter ce dernier. Réaliser une analyse des écarts entre les compétences actuelles et les compétences requises pour élaborer une stratégie visant à combler ces écarts.
- Structurer ou restructurer les bilans de performance pour intégrer des compétences propres à certains postes, des objectifs réalisables qui correspondent au plan stratégique de l'organisation, et des grilles salariales pour les professionnels spécialisés comme les analystes de données.
- Accompagner et développer les compétences des collaborateurs en poste, ce qui entraîne un minimum de perturbations et incorpore les nouvelles compétences requises aux connaissances organisationnelles existantes.
- Acquérir en permanence de nouvelles compétences sur le marché. Rechercher des candidats issus d'horizons divers, pas uniquement des diplômés en comptabilité et en finance. Considérer les prestataires de services externes comme une ressource pour obtenir rapidement les compétences nécessaires pour faire face à des risques complexes et spécialisés.
- Établir un programme efficace d'accueil et de transfert de connaissances.

Analyse de données

L'analyse des données est le processus qui consiste à collecter et analyser des données afin d'utiliser les résultats pour prendre de meilleures décisions *(Internal Auditing, 4th edition, 11-2, Internal Audit Foundation,* 2017). Les organisations produisent des dépôts de données de plus en plus grands à partir de leurs opérations. A cet égard, les enjeux clés pour l'audit interne sont de deux ordres. Le premier est d'aider le Conseil et la direction générale à comprendre comment ces données sont recueillies, gérées, protégées et exploitées à des fins opérationnelles. Le second est la manière d'exploiter ces données, de plus en plus nombreuses, du point de vue de l'audit interne en appliquant des outils d'analyse pour évaluer les processus, en automatisant par conséquent les missions d'audit de routine pour libérer du temps à consacrer aux domaines de risques émergents (cf. Risques à cibler : les sujets incontournables de l'audit interne en 2018).

En bref, l'analyse des données décompose de grands volumes de données et les recompose sous une forme plus exploitable, permettant ainsi de les "faire parler". Grâce à ces informations, l'audit interne peut, sur l'ensemble d'une population, analyser les risques et les corrélations potentielles, fournir des points de vue et une vision prospective, et rendre compte des problématiques qui préoccupent et intéressent les parties prenantes. La gestion des analyses de données, et des risques y afférents, peut être décourageante. Extraire des informations significatives de ces données, et mettre ce savoir en pratique, est parfois plus facile à dire qu'à faire. Pour que les analyses de données soient efficaces, les talents, formats, processus et technologies adéquats doivent être en place.

La direction générale et le Conseil doivent prendre conscience que ces immenses quantités de données exposent l'organisation à des risques financiers et extra-financiers. Plusieurs domaines de risques doivent être traités dans toute initiative d'analyse (cf. Understanding and Managing the Risks of Analytics) :

- **Risques liés à la qualité des données et des informations** — Les décideurs requièrent des données qui facilitent la compréhension de la complexité de l'organisation. Toutes les données et les informations doivent être accompagnées de définitions et de normes de qualité claires.
- **Risques liés à la conformité des données et des informations** — La non conformité avec les exigences d'un agent mandaté et reconnu (en général au niveau national, fédéral ou international) peut avoir des conséquences négatives comme une amende, une charge de travail supplémentaire ou la mise en cause de la responsabilité personnelle.
- **Risques de gouvernance liés aux données et aux informations** — Les données et les informations doivent être contrôlées attentivement en utilisant les principes et processus de management des risques à des niveaux appropriés pour assurer leur confidentialité, leur sécurité, leur qualité, et leur auditabilité.
- **Risques d'utilisation inappropriée ou prématurée de l'analyse** — L'analyse ne sera pas utile s'il n'y a pas suffisamment de temps pour recueillir, traiter et interpréter les données ; s'il n'y a pas de contexte ou d'antécédents liés aux décisions ou si les données historiques sont erronées; ou encore si les variables clés ne peuvent être mesurées ou comportent des degrés élevés d'incertitude.
- **Risques d'impact contre-culturel** — Imposer des initiatives d'analyse dans une culture d'entreprise qui n'est pas orientée sur les données peut représenter un risque important pour les responsables. Celles-ci devraient inclure une évaluation du système de prise de décision et du degré d'orientation « données » de la culture.
- **Risques liés à l'éthique des données** — Les initiatives d'analyse de données devraient s'aligner sur les valeurs clés, le processus de prise de décision et les comportements de l'organisation. Des contrôles devraient être instaurés pour assurer la collecte et l'utilisation éthiques des données.

L'audit interne doit toujours être conscient des dangers que peuvent entraîner des projets de *big bata* pour les organisations, notamment si l'équipe manque de compétences. La demande d'analyse de données est en hausse et bientôt, si ce n'est pas déjà le cas, elle fera partie intégrante de chaque organisation. Même s'il est important pour les organisations de participer à des projets de *big data* pour rester concurrentielles et ne pas être à la traîne, certains risques doivent être pris en compte :

- la sécurité des données,
- la confidentialité,
- les coûts,
- les données non fiables, invalides, insuffisantes et non pertinentes,
- les processus analytiques non fiables, invalides, insuffisants ou non pertinents.

Les technologies changent le monde dans lequel nous vivons à un rythme fulgurant et les conséquences sont pour le moins frustrantes si nous ne sommes pas correctement préparés. Elles génèrent des quantités de données importantes dont l'audit interne peut se servir pour évaluer les risques plus précisément, améliorer la prestation de missions d'audit et augmenter le niveau d'assurance fournie.

Des études de cas menées récemment ont identifié les principaux avantages de l'analyse de données pour l'audit interne parmi lesquels un gain d'efficience et d'efficacité, un niveau d'assurance accru, un accent mis sur les risques stratégiques, un périmètre d'audit élargi et des économies importantes de temps et de coûts sur le long terme. Cependant, pour bénéficier de ces avantages, l'audit interne doit évaluer la mesure dans laquelle le programme d'analyse de données sert ses principaux objectifs et ses activités envisagées.

L'analyse de données est un outil indispensable pour l'audit interne car elle peut extirper des informations enfouies dans les données et permettre des tests plus efficients et efficaces. Bon nombre d'équipes d'audit interne n'ont pas encore adopté les technologies d'analyse de données les plus sophistiquées et continuent de s'appuyer principalement sur des systèmes et des applications de tableur. Le soutien du comité d'audit est essentiel. L'audit interne devrait s'assurer que ce dernier connaît l'importance de l'analyse de données (cf. Data Analytics: Is it Time to Take the First Step?).

Pour créer ou améliorer un programme d'analyse de données, les responsables de l'audit interne devraient discuter des résultats souhaités avec les parties prenantes, définir des objectifs d'analyse et déterminer les *compétences* et les technologies requises.

L'un des principaux obstacles à l'élaboration d'un programme efficace d'analyse des données – et un risque permanent pour l'audit interne – est l'insuffisance des compétences pour traiter le *big data*. En raison d'un déficit de qualification

dans cette spécialisation, les programmes d'analyse de données de l'audit interne pourraient ne pas être optimaux, pas nécessairement à cause du programme en lui-même, mais plutôt parce que son potentiel n'est pas exploité pleinement. Comme pour toute nouvelle initiative, les projets de *big data* comportent un élément de risque. Si l'expertise nécessaire pour gérer les données fait défaut, cela augmente d'autant plus l'élément de risque.

Objectifs

- L'audit interne a une connaissance approfondie de l'analyse des données et des systèmes d'information et sait comment les technologies de pointe peuvent rendre l'audit interne plus efficient et efficace.
- L'audit interne évalue dans quelle mesure la direction générale fait face aux nouveaux risques liés à l'utilisation accrue de l'analyse de données.
- L'audit interne utilise les capacités avancées des programmes d'analyse de données au profit de l'organisation (par exemple, validation et suivi des schémas et des comportements à haut risque, appréciation et pertinence des processus d'évaluation des risques spécifiques à l'organisation, etc.).
- L'audit interne tire parti des technologies pour identifier des anomalies et des schémas de risque de fraude en amont et communique les principaux constats.
- L'audit interne tire parti des technologies pour améliorer la couverture globale des risques de l'organisation pour un temps de travail et un coût réduits.

Partiellement adapté de : First Steps in Building a Data Analytics Program for Your Internal Audit Team.

Actions

- Déterminer les résultats d'analyses qui servent le mieux les objectifs de l'audit interne, en décidant quels sont les besoins fondamentaux et spécifiques pour le programme d'analyse de données.
- Comprendre les avantages que les programmes d'analyse peuvent apporter à l'organisation et à l'audit interne en termes d'innovation et d'opportunité. Identifier les compétences requises pour mettre en œuvre les programmes de manière optimale et profiter des avantages.
- Considérer l'analyse des données comme un élément clé pour l'activité et adapter les missions d'audit pour augmenter la qualité et la soutenabilité des démarches de conformité et de contrôle interne de l'organisation.
- Collaborer avec le management sur des règles spécifiques, des points de données, des codes et des hypothèses dans le programme qui détecteront avec précision les irrégularités ou les schémas de fraude.

Cybersécurité

Qu'il s'agisse des violations de données incessantes dont les organisations sont victimes ou du nombre incalculable d'usurpations d'identité, les cybercriminels, sophistiqués et bien financés, sont des adversaires redoutables. L'interconnectivité fait de notre monde complexe une proie parfaite pour les cybercriminels. Les techniques qu'ils utilisent continuent de se développer et d'évoluer, tant et si bien qu'il est devenu difficile de les suivre.

Lancer un plan de défense contre les cyberattaques et s'assurer que ce plan est efficace est une activité à plein temps. La question n'est pas si mais quand une attaque va se produire. Il y a une grande différence entre la sensibilisation et la préparation aux cyber-risques. Nous sommes tous conscients des risques ; nous y sommes confrontés tous les jours. Toutefois, la préparation implique la capacité à déjouer entièrement une tentative d'attaque, ou à résister à une attaque en s'en tirant avec relativement peu ou pas de dégâts. Pour que les organisations bénéficient ne serait-ce que d'un soupçon de protection contre le désastre provoqué par une violation, elles doivent être capables de résister, réagir et se remettre des cyberattaques. Elles doivent être cyber-résilientes.

Alors que l'inquiétude suscitée par les problématiques de cybersécurité (par exemple le piratage, les intrusions, le *spear-phishing*, l'espionnage économique, etc.) augmente, les parties prenantes exigent une plus grande visibilité sur les programmes de gestion des risques de cybersécurité de leur organisation et les administrateurs veulent que l'audit interne réalise un examen complet, objectif et indépendant des cyber-risques et des cyber-programmes. Par conséquent, l'audit interne doit également connaître les risques potentiels et jouer un rôle important dans la cyber-résilience.

Malheureusement, le risque de cybersécurité ne se limite pas aux menaces externes. Certaines menaces potentielles peuvent résulter des actions de collaborateurs ou de partenaires. De ce fait, une composante essentielle de la cyber-résilience est la gestion adéquate et efficace de la culture d'une organisation, ainsi que l'évaluation des risques qu'elle comporte. Lorsqu'ils envisagent la culture, les administrateurs incluent également la culture du risque, car elle constitue la base de toutes les décisions, de la conduite des affaires et de la prise de risques dans toute l'organisation. L'audit interne peut évaluer la culture du risque dans le cadre d'audits financiers et opérationnels classiques en collectant des données et en procédant à des examens informels.

En tant que chef de file, l'audit interne peut aider le management à mieux comprendre l'efficacité des contrôles de cybersécurité dans tous les domaines, y compris la mesure dans laquelle la culture d'une organisation influe sur les exigences, les processus et les capacités. La culture stimule la productivité, les valeurs, les comportements et les pratiques au sein d'une organisation, et est façonnée et maintenue par de nombreux facteurs. L'audit

interne peut donc évaluer la culture du risque de la même manière qu'il évalue d'autres domaines de l'organisation (cf. Internal Audit Future Trends). L'audit interne peut maximiser sa valeur en comprenant comment évaluer la culture et en formant le management sur son importance.

Afin de surmonter les cyber-risques, y compris dans leurs aspects culturels, il est essentiel que l'équipe de direction définisse des mesures de précaution et les mette en place au moyen de programmes de formation et de sensibilisation, puis s'assure du changement des comportements. Les collaborateurs, les fournisseurs, les partenaires et les prestataires doivent être formés et pleinement conscients de ce que l'on attend d'eux en ce qui concerne les mesures et les protocoles de cybersécurité.

Les stratégies d'évaluation des risques de l'audit interne devraient être élaborées en tenant compte de tous les risques propres à la cybersécurité et assurer le respect des politiques et des dispositifs de contrôle interne. L'audit interne doit développer une approche d'audit spécifique qui réponde aux besoins de l'organisation et de ses parties prenantes dans tous les domaines pouvant être touchés par des problèmes de cybersécurité. Pour être efficace, la mise en place, a minima, d'activités de contrôle, d'un environnement de contrôle, d'une évaluation des risques, d'une communication, d'un suivi, ainsi que d'un cadre d'évaluation des mesures de cybersécurité est nécessaire (cf. Risque à cibler : les sujets incontournables de l'audit interne en 2018).

En tant que troisième ligne de maîtrise, l'audit interne devrait travailler avec la direction générale et le Conseil à l'élaboration de stratégies et de politiques de cybersécurité afin d'améliorer la capacité de l'organisation à identifier et à atténuer les risques de cybersécurité ; tirer parti des relations avec le comité d'audit et le Conseil, en veillant à ce qu'ils restent impliqués; et s'assurer que le risque de cybersécurité est formellement intégré dans le plan d'audit, avec les compétences nécessaires (en interne ou en co-traitance) pour exécuter le plan. Les technologies et tendances émergentes influent sur le profil de risque de cybersécurité d'une organisation. Pour cette raison, l'audit interne devrait également se tenir au courant des dernières avancées technologiques et évaluer le niveau de vulnérabilité de l'organisation et ses activités à risque à l'aune du plan de cybersécurité choisi.

Objectifs

- L'organisation a une culture de cyber-résilience.
- L'audit interne apporte des éléments clés essentiels à l'analyse de la cybersécurité et à la préparation :
  - Protection et détection : L'audit interne fournit une approche globale permettant d'identifier les vulnérabilités de l'organisation et intègre l'analyse de données dans son domaine de responsabilité, permettant de signaler toute anomalie.

« Les dirigeants n'ont pas besoin d'être des technologues pour jouer un rôle important dans le contrôle des cyber-risques – mais chaque administrateur peut avoir l'opportunité d'améliorer l'efficacité des pratiques de cybersurveillance ».

NACD Director's Handbook on Cyber-Risk Oversight, National Association of Corporate Directors (NACD), 2017

Source : The Value of Visibility: Cybersecurity risk management examination

Point d'attention

Norme de l'IIA 2130 : Contrôle

L'audit interne doit aider l'organisation à maintenir un dispositif de contrôle approprié en évaluant son efficacité ainsi que son efficience et en encourageant son amélioration continue.

2130.A1 – L'audit interne doit évaluer la pertinence et l'efficacité du dispositif de contrôle choisi pour faire face aux risques relatifs à la gouvernance, aux opérations et systèmes d'information de l'organisation. Cette évaluation doit porter sur les aspects suivants :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats.

- Continuité de l'activité : l'audit interne donne des conseils et collabore avec le management dans le cadre de la planification et de la résolution de scénarios de risques susceptibles d'avoir une incidence sur les opérations en cours, notamment les cyberattaques, les catastrophes naturelles ou la succession.
- Gestion/communication de crise : l'audit interne aide à la planification de la gestion de crise et à la préparation à la communication de crise en réalisant des contrôles d'assurance centrés sur l'efficacité et la rapidité, et en menant des analyses et des critiques des plans exécutés.
- Amélioration continue : l'audit interne apporte une valeur ajoutée en fournissant des points de vue et en améliorant les stratégies et les protocoles pour renforcer la préparation aux cyberattaques.

Actions

- Évaluer la culture organisationnelle en ce qui concerne la cyber-résilience.
- Effectuer des évaluations de risques des modèles de sécurité et des processus de cybersécurité et faire des recommandations d'améliorations.
- Effectuer des tests d'intrusion avec des prestataires SI et externes pour évaluer leur capacité à se conformer aux protocoles établis.
- Effectuer des analyses d'écart en matière de cyberrésilience, recommander des mesures de remédiation et assurer le suivi des activités de remédiation.
- Influencer la culture en faisant du suivi et de la réponse en matière de cybersécurité des priorités absolues.
- Assurer que le plan de continuité des opérations est testé périodiquement et que des mesures correctives sont prises pour toute anomalie identifiée.
- Mettre en œuvre et encourager une cyber-culture et une culture du risque fortes dans toute l'organisation, ce qui, avec le temps, renforcera les mesures et les protocoles de cybersécurité.

Réglementations

À l'échelle mondiale, les organisations font face à des exigences réglementaires nouvelles ou modifiées, conçues en partie pour protéger les consommateurs ou l'intérêt public. Les réglementations les plus médiatisées portent sur les risques et contrôles financiers ainsi que sur la protection et la sécurité des données personnelles et ont un impact sur les organisations dans tous les secteurs.

Cryptomonnaies

Selon CNBC, les cryptomonnaies pourraient dépasser la barre du billion de dollars en termes de valeur, à la suite d'une récente vente massive de ces monnaies digitales. La valeur du Bitcoin est volatile : Début 2018, elle

oscillait entre 6 000 $ et 10 000 $. Selon Thomas Glucksmann, responsable du marketing de la plateforme d'échanges Gatecoin, « la reconnaissance réglementaire croissante des bourses de cryptomonnaies, l'entrée de capitaux institutionnels et des évolutions technologiques majeures contribueront au rebond du marché et pousseront les prix de la cryptomonnaie à atteindre de nouveaux sommets cette année. Rien n'empêche le Bitcoin de franchir le seuil des 50 000 $ d'ici décembre (2018) ».

Alors que, dans le monde entier, les grands établissements financiers s'intéressent de plus en plus à la technologie *blockchain* et au *trading* des cryptomonnaies, ils doivent trouver le moyen de gérer les conflits qui peuvent survenir lorsque leurs collaborateurs échangent des monnaies digitales sur leurs comptes personnels. La flambée des prix des monnaies digitales n'a pas seulement attiré l'attention des investisseurs et des banques, mais aussi des fonctions de conformité. Des conflits pourraient apparaître si les collaborateurs qui investissent ou souhaitent investir dans la crypto-monnaie bénéficient d'un avantage indu. Généralement, ils doivent obtenir une autorisation avant de négocier des valeurs qui représentent un conflit d'intérêts. Cependant, les politiques habituelles sont beaucoup plus difficiles à appliquer avec les cryptomonnaies, car les transactions sont effectuées à travers un réseau fragmenté, parfois de manière anonyme, ce qui complique leur suivi. De plus, l'absence de règles claires émanant des régulateurs mondiaux, ne facilite pas la tâche aux établissements financiers pour édicter les leurs. Certains considèrent les cryptomonnaies comme des marchandises, et d'autres assimilent certaines cryptomonnaies à des valeurs, sans spécifier lesquelles. L'explosion récente de la volatilité du Bitcoin et d'autres devises digitales préoccupe les régulateurs internationaux, si bien que des réglementations ciblées pourraient être mises en place (cf. Compliance Officers Sweat as cryptocurrency Trades Go Mainstream).

Réglementations internationales sur la protection des données

Un certain nombre de gouvernements mettent en œuvre des réglementations plus strictes sur la protection des données personnelles. C'est notamment le cas de l'Union européenne (UE) et de la Chine.

Après quatre années de préparation et de débat, le règlement général de l'UE sur la protection des données (RGPD), qui remplace la Directive 95/46 / CE sur la protection des données, a été approuvé par le Parlement européen en avril 2016. Le RGPD entrera en vigueur en mai 2018, alors que les violations deviennent plus importantes, plus intrusives et plus coûteuses, année après année. Les violations de données ont considérablement augmenté en 2017, dépassant l'augmentation de 40 % enregistrée entre 2015 et 2016. (Pour plus de détails, voir le tableau « les violations de données en 2017 », page 13).

« Le RGPD et ses répercussions ont une importance croissante. En termes de missions d'assurance, le comité d'audit souhaite dans un premier temps que nous évaluions le dispositif lui-même, et qu'ensuite nous élaborions notre propre programme pour s'assurer régulièrement que l'organisation a mis en place les processus nécessaires afin de rester en conformité ».

Responsable de l'audit interne dans un groupe bancaire multinational

Source : Risques à cibler : les sujets incontournables de l'audit interne en 2018

Bien que de nombreuses entreprises disposent de politiques de protection des données conformes à l'ancienne directive, le nouveau RGPD contient un certain nombre de nouvelles protections relatives aux données de l'UE et prévoit d'infliger aux responsables du traitement des données et aux sous-traitants des amendes ou des pénalités pour non-conformité dès son entrée en vigueur. Autrement dit, toute organisation (locale ou internationale) qui exerce son activité en Europe ou gère les données personnelles de résidents de l'UE doit se conformer aux nouvelles règles.

Pour les manquements les plus graves aux principales dispositions, les régulateurs ont le pouvoir d'imposer une amende d'un montant pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial de l'année précédente. Le RGPD prévoit des amendes par paliers. (Par exemple, les entreprises peuvent être condamnées à une amende de 2 % pour ne pas avoir tenu des registres de leurs activités [article 28], ne pas avoir notifié une violation à l'autorité de contrôle ou à la personne concernée ou ne pas avoir mené une analyse d'impact).

Il est important de noter que ces règles s'appliquent aussi bien aux responsables du traitement des données qu'aux sous-traitants, ce qui signifie que les serveurs *cloud* ne seront pas exemptés de l'application du RGPD. Les autres exemples qui entrent dans cette catégorie sont le non-respect des principes fondamentaux du traitement des données personnelles, la violation des droits des personnes concernées et le transfert de données personnelles vers un pays tiers ou une organisation internationale qui n'offre pas un niveau adéquat de protection des données. (cf Règlement général de l'UE sur la protection des données).

Même la définition et les conditions du « consentement » sont considérablement restreintes. Auparavant, les responsables du traitement des données étaient autorisés à s'appuyer sur le consentement implicite et l'*« opt-out »* dans certaines circonstances. À compter du 25 mai 2018, le RGPD durcira les conditions du consentement. Les entreprises ne pourront plus avoir recours à des Termes & Conditions interminables et truffés de jargon juridique, dans la mesure où la demande de consentement devra être communiquée de manière intelligible et facile d'accès, expliquant clairement à quoi serviront les données demandées.

Le demande de consentement doit être présentée sous une forme qui la distingue clairement des autres questions et formulée en des termes clairs et simples. Il doit être aussi facile de retirer que de donner son consentement. En outre, les personnes concernées ont le droit d'obtenir que leurs données personnelles soient effacées et ne soient plus traitées dès lors qu'elles ont retiré leur consentement (cf. The Top 10 Operational Impacts of the EU's General Data Protection Regulation).

Le RGPD affectera de manière significative les travaux de l'Allemagne en matière de cybersécurité. En mai 2017, le législateur allemand a adopté

Les violations de données en 2017

Mois	Organisation	Violation / faille
8 janvier 2017	E-Sports Entertainment Association (ESEA)	1 503 707 comptes enregistrés dans la base de données et contenant des informations personnelles/privées ont été piratés.
2 février 2017	Xbox 360 ISO et PSP ISO	1,2 million d'inscrits sur le forum Xbox 360 ISO et 1,3 million d'inscrits sur le forum PSP ISO ont été touchés. Des informations personnelles/privées ont été volées.
15 mars 2017	Dun & Bradstreet	Plus de 33 millions de contacts d'entreprises partagés sur le Web, y compris le Ministère de la Défense et le service postal des États-Unis. Des informations personnelles/privées ont été divulguées.
6 avril 2017	FAFSA : IRS Data Retrieval Tool	Les informations personnelles / privées d'environ 100 000 contribuables/étudiants pourraient avoir été volées.
10 mai 2017	Centre hospitalier Bronx Lebanon	Les informations extrêmement confidentielles d'au moins 7 000 patients pourraient avoir été piratées entre 2014 et 2017, y compris des addictions, des diagnostics de santé mentale et médicale, le statut VIH et des rapports d'agression.
20 juin 2017	Deep Root Analytics	Environ 198 millions de citoyens américains ont été touchés, car Deep Root Analytics, employé par le Comité national républicain, a stocké des informations privées/personnelles sur un serveur *cloud* non protégé par mot de passe et donc exposé pendant plus de deux semaines.
13 juillet 2017	Verizon	Les informations de 14 millions d'abonnés ont été exposées, car les dossiers clients étaient conservés sur un serveur non sécurisé ; les données obtenues étaient des fichiers log, générés lorsque des clients contactaient Verizon par téléphone.
30 août 2017	Online Spambot	711 millions d'adresses e-mail et mots de passe ont été récoltés à partir d'un serveur non sécurisé.
7 septembre 2017	Equifax	143 millions de clients pourraient avoir été touchés en raison de l'exploitation par des pirates d'un point faible dans le logiciel du site Web ; des informations personnelles/privées ont été dérobées, y compris les numéros de sécurité sociale et les numéros de carte de crédit.
12 octobre 2017	Hyatt Hotels	Accès non autorisé aux informations de paiement, y compris les numéros de carte de crédit, les codes de vérification interne et les noms de titulaires, relatives à des cartes de débit et de créditutilisées *(swipées)* dans 41 hôtels dans 11 pays différents.
21 novembre 2017	Uber	Les renseignements personnels de 57 millions de chauffeurs et de clients ont été subtilisés, y compris les noms, adresses électroniques et numéros de téléphone.
10 décembre 2017	TIO Networks (PayPal)	Les identités de plus de 1,6 million de clients ont été compromises, y compris des informations de compte bancaire et de carte de paiement, des mots de passe, des noms d'utilisateur et des numéros de sécurité sociale.

Adapté de : 2017 Data Breaches – The Worst So Far

Point d'attention

Norme de l'IIA 2120 : Management des risques

L'audit interne doit évaluer l'efficacité des processus de management des risques et contribuer à leur amélioration.

2120.A1 – L'audit interne doit évaluer les risques afférents à la gouvernance, aux opérations et aux systèmes d'information de l'organisation au regard de :

- l'atteinte des objectifs stratégiques de l'organisation ;
- la fiabilité et l'intégrité des informations financières et opérationnelles ;
- l'efficacité et l'efficience des opérations et des programmes ;
- la protection des actifs ;
- le respect des lois, règlements, règles, procédures et contrats.

une version révisée de la loi fédérale sur la protection des données, qui entrera en vigueur en même temps que le RGPD le 25 mai 2018. Reconnue pour ses lois nationales rigoureuses sur la protection des données, avec des amendes allant jusqu'à 300 000 €, l'Allemagne passe désormais à des normes strictes de cybersécurité et assigne la responsabilité de protéger les utilisateurs et de sécuriser les informations électroniques à des prestataires de services et des exploitants d'infrastructures critiques. La nouvelle loi contient 85 dispositions, dont plusieurs renvoient au RGPD de l'UE. Les exploitants d'infrastructures critiques doivent mettre en œuvre des garanties organisationnelles et techniques appropriées et d'autres mesures, en tenant compte de l'état des connaissances, dans les deux ans suivant l'entrée en vigueur de la législation secondaire spécifiant ces garanties. De plus, les exploitants d'infrastructures critiques doivent régulièrement prouver qu'ils répondent aux exigences de sécurité et notifier immédiatement le *Bundesamt für Sicherheit in der Informationstechnik* (BSI) de toute perturbation significative affectant la disponibilité, l'intégrité, l'authenticité et la confidentialité de leurs systèmes, composants et processus informatiques, pouvant ou ayant entraîné l'échec ou une dégradation du fonctionnement de l'infrastructure critique qu'ils exploitent (cf. What You Need to Know About Germany's Cybersecurity Law).

Alors que la Chine disposait déjà de lois, règles et réglementations strictes en matière de sécurité de l'information, elle a introduit une loi plus détaillée qui fait le lien entre la cybersécurité et la protection des données (entrée en vigueur en juin 2017) et fusionne les dispositions du RGPD. À maints égards, la Loi sur la cybersécurité de la République populaire de Chine (CSL) concorde avec le RGPD (cf. Risques à cibler : les sujets incontournables de l'audit interne en 2018). La CSL a apporté des modifications qui se focalisent davantage sur la protection des données personnelles et de la vie privée, et normalise la collecte et l'utilisation de ces données. Par exemple, auparavant, les entreprises étrangères transféraient des informations en dehors de la Chine. Aujourd'hui, la loi stipule que les données sensibles doivent être stockées dans le pays, et prévoit des sanctions sévères en cas de violation de la loi, notamment la suspension des activités commerciales. Les amendes peuvent atteindre 1 000 000 RMB (Pour plus de détails, voir « Modifications de la CSL », page 15).

Mais la CSL ne fait pas l'unanimité. Comme le rapportait le New York Times en mai 2017, « une coalition de groupes de pression représentant des entreprises européennes, américaines et asiatiques ont demandé à la Chine de retarder la mise en application de la loi, tandis que la Chambre de commerce de l'UE en Chine a demandé un délai supplémentaire pour permettre aux entreprises de se conformer en raison d'« obligations de conformité importantes ».

Qu'elles opèrent au sein de l'UE, en Chine, ou dans d'autres pays renforçant leur réglementation sur la protection des données, les organisations en ressentent les effets. Les administrateurs encouragent leurs organisations à adopter des cadres de gouvernance améliorés, et sont soumis à la pression des régulateurs, des

investisseurs et des autres parties prenantes qui les tiennent pour responsables de l'efficacité de leurs processus globaux (cf. Of Corporate Governance, Risk Management, and Internal Audit). Les nouvelles réglementations entraînent une augmentation des coûts et exercent une pression sur les organisations en compliquant les processus de gouvernance, de contrôle et de management des risques.

À mesure que la pression sur les administrateurs s'intensifie, l'audit interne en pâti également. En effet, les organisations attendent beaucoup de ce dernier. Elles reconnaissent la nécessité des conseils et de l'assurance fournis par l'audit interne pour leur permettre de transformer les forces perturbatrices en opportunités tout en s'adaptant aux nombreux changements réglementaires (cf. KPMG Internal Audit: Top 10 Key Risks in 2016).

Modifications de la CSL

Article	Version finale	Modification importante
31	En matière de cybersécurité, l'État met l'accent sur la protection des infrastructures d'information critiques dans les services de communication, l'énergie, le transport, l'eau, la finance, le service public, l'e-gouvernement, ainsi que dans d'autres infrastructures d'information critiques pouvant nuire sévèrement à la sécurité nationale, à l'économie nationale et à l'intérêt public en cas de destruction, de fonctionnalité perdue ou de divulgation de données.	Cet article clarifie les secteurs dans lesquels la protection de l'infrastructure d'information critique sera prioritaire.
43	Les particuliers sont en droit de demander aux opérateurs de réseau de corriger les erreurs dans les informations personnelles qu'ils collectent ou stockent. ***Les opérateurs de réseau devraient prendre des mesures pour supprimer ou corriger les erreurs.***	Cet article donne aux citoyens plus de droits pour protéger leurs informations personnelles, et renforce l'obligation des opérateurs de réseau de corriger les erreurs en temps opportun.
46	Les particuliers ou les organisations ***sont responsables de l'utilisation de leurs réseaux,*** et ne doivent pas créer de sites Web ou de groupes de communication à des fins frauduleuses ou pour toute autre activité illégale.	Cet article souligne que les particuliers et les organisations sont responsables de l'utilisation de leurs réseaux.
76(5)	Les « informations personnelles » désignent toutes sortes d'informations, enregistrées électroniquement ou par d'autres moyens, qui permettent de déterminer l'identité de personnes physiques indépendamment ou en combinaison avec d'autres informations, notamment le nom d'une ***personne physique,*** sa date de naissance, son numéro de sécurité sociale, ses informations biométriques personnelles, son adresse et son numéro de téléphone.	Cet article élargit le périmètre de la protection des informations personnelles des « citoyens » aux « personnes physiques ».
63	Les personnes qui enfreignent l'article 27 de la loi et se livrent à des activités qui mettent en péril la cybersécurité peuvent être détenues pendant 5 à 15 jours et peuvent être condamnées à une amende allant de ***100 000 RMB à 1 000 000 RMB,*** selon la gravité de l'affaire.	La peine maximale pour violation de la loi sur la cybersécurité a été portée à 1 000 000 RMB.

Source : Overview of China's Cybersecurity Law

Point d'attention

Norme de l'IIA 2210 : Objectifs de la mission

Les objectifs doivent être précisés pour chaque mission.

> **2210.A3 –** Des critères adéquats sont nécessaires pour évaluer la gouvernance, le management des risques et le dispositif de contrôle. Les auditeurs internes doivent déterminer dans quelle mesure le management et/ou le Conseil a défini des critères adéquats pour apprécier si les objectifs et les buts ont été atteints. Si ces critères sont adéquats, les auditeurs internes doivent les utiliser dans leur évaluation. S'ils sont inadéquats, les auditeurs internes doivent identifier, à travers une discussion avec le management et le Conseil, les critères d'évaluation appropriés.

Norme de l'IIA 2050 : Coordination et utilisation d'autres travaux

Afin d'assurer une couverture adéquate et d'éviter les doubles emplois, le responsable de l'audit interne devrait partager des informations, coordonner les activités, et envisager d'utiliser les travaux des autres prestataires internes et externes d'assurance et de conseil.

Pour surmonter ces perturbations, il est essentiel d'atteindre un équilibre entre gouvernance, management des risques, conformité réglementaire et performance afin de protéger et améliorer la valeur de l'organisation et son efficacité opérationnelle.

Objectifs

- Clarifier l'appétence pour le risque lors de l'évaluation des projets et des stratégies.
- Sensibiliser toute l'organisation aux réglementations nationales et internationales actuelles.
- Établir des mesures de mise en conformité avec les réglementations nationales et internationales actuelles.
- Coordonner les prestataires d'assurance internes et externes.

Actions

- Comprendre les cadres de conformité internationaux et les normes d'assurance.
- Effectuer un inventaire des autorités de régulations existantes et de leurs exigences.
- Évaluer l'approche de l'organisation pour la gestion de ses activités de conformité globales, y compris l'intégration d'organisations nouvellement acquises.
- Évaluer la réponse de l'organisation face à des cas notables de non-conformité.
- Examiner les programmes de formation sur la conformité et évaluer la pertinence des rôles respectifs.
- Se coordonner avec les prestataires d'assurance internes et externes pour assurer une couverture adéquate et minimiser les doubles emplois.
- Élaborer des communications adaptées aux intérêts et aux priorités de l'organisation pour favoriser une culture de la conformité.
- Évaluer l'attribution par l'organisation des responsabilités en matière de conformité aux réglementations.

Réponse aux perturbations

À chaque jour son innovation. Les technologies actuelles changent constamment : plus rapides, plus fortes, plus grandes (et plus petites), elles vont plus loin, et sont plus intenses. Comme jamais auparavant. Quotidiennement, les auditeurs internes sont confrontés à de nouvelles opportunités de fournir des points de vue et une vision prospective aux parties prenantes, mais ils manquent peut-être de compétences liées à l'innovation telles que le raisonnement critique et la créativité. Par conséquent, sans innovation, ils se retrouvent incapables de gérer les imprévus et enclins à l'autosatisfaction. Les auditeurs internes doivent adapter

leurs méthodes d'utilisation des technologies, pour devenir agiles et proactifs, et être en mesure de changer rapidement de direction pour suivre le rythme de l'innovation.

Alors que les innovations, telles que les nouvelles technologies, offrent à l'audit interne des opportunités considérables pour réaliser des missions d'audit, elles s'accompagnent souvent de nouveaux risques, de nouvelles menaces et de nouvelles disruptions qui viennent s'ajouter aux préoccupations de l'audit interne. Par exemple, au lieu de se concentrer uniquement sur les risques (leur rôle traditionnel), les auditeurs internes doivent désormais être en mesure d'identifier rapidement les disruptions potentielles et de déterminer celles qui requièrent une attention immédiate ou supplémentaire.

L'une des principales raisons pour lesquelles une organisation devrait innover est pour se démarquer de la concurrence. Or, l'audit interne peut être à l'avant-garde dans ce domaine. Selon l'enquête *Pulse of Internal Audit 2018* de l'IIA Amérique du Nord, l'innovation place l'audit interne face à deux alternatives : reconsidérer ses capacités à remplir un rôle de plus en plus important dans l'organisation, ou s'en tenir à d'anciennes pratiques et les reproduire dans le futur. Cette deuxième option ne peut conduire qu'à l'échec. Par conséquent, l'audit interne doit être ouvert à des idées créatives (voire radicales) et être prêt à se concentrer sur la gestion efficace des risques liés à l'innovation.

Cette transition ne se fera pas sans difficulté. La direction générale peut être réticente à l'idée de faire les choses différemment, les budgets peuvent être limités par l'environnement économique, et le nombre de candidats dotés des compétences requises peut être insuffisant. La bonne nouvelle, c'est que l'audit interne n'est pas seul. Il peut apprendre d'autres unités opérationnelles, organisations ou fonctions d'audit interne qui ont déjà développé des techniques spécifiques pour gérer le processus d'innovation.

L'innovation, lorsqu'elle est adoptée correctement, est extrêmement utile à l'audit interne et à l'ensemble de l'organisation. Elle permet :

- la réduction des coûts ;
- l'augmentation de la valeur ;
- une croissance en hausse et une meilleure performance ;
- le lancement des produits et des services dans des délais plus brefs ;
- l'amélioration de l'expérience et de la satisfaction du client ;
- une plus grande flexibilité et agilité de l'organisation ;
- l'augmentation de la satisfaction des parties prenantes.

L'innovation permet non seulement à l'audit d'être plus efficace, mais elle soutient directement l'agilité en permettant de répondre à une disruption de manière plus rapide, plus intelligente et plus ciblée (cf. 2018 North American Pulse of Internal Audit: The Internal Audit Transformation Imperative). La présidente du Conseil

« Je crois sincèrement que l'audit interne joue un rôle essentiel dans la réussite de nos organisations. Mais je crois également que pour être à la hauteur de la tâche, nous devons revoir nos engagements en faveur de l'innovation. L'innovation doit être au cœur de la mission de l'audit interne s'il veut rester en phase avec les évolutions dans nos propres organisations et au-delà ».

Shannon Urban, Présidente du Conseil de l'IIA Amérique du Nord (2017 – 2018)

Source : Internal Auditor

de l'IIA Amérique du Nord, Shannon Urban, encourage l'innovation dans l'audit interne, la considérant à la fois comme un moteur de sa croissance et comme un prérequis pour satisfaire les besoins en constante évolution des parties prenantes. Elle peut être un peu délicate et frustrante, mais elle suit son cours et exige de l'engagement et du courage. L'innovation peut aussi s'avérer très enrichissante. Si l'audit interne veut comprendre ses parties prenantes et les servir au mieux à l'avenir, accepter l'innovation est la seule option (cf. The Innovative Internal Auditor).

Objectifs

- L'audit interne identifie les changements dans l'environnement économique.
- L'audit interne vise à développer une culture de l'innovation et à renforcer les capacités et la performance.
- L'audit interne cible des meilleures pratiques et des améliorations réalisables grâce à l'innovation.
- L'audit interne œuvre pour plus d'efficacité grâce à l'innovation.

Actions

- Concevoir et mettre en œuvre de nouvelles idées, faire de l'innovation un fondement de la pratique de l'audit interne.
- Jouer un rôle de leader, anticiper les perturbations, surveiller les changements dans l'environnement économique, et proposer une gamme de réponses plus larges.
- Développer des relations et investir en elles. Rester connecté à l'activité et prendre conscience des innovations qui sont menées.
- Clarifier le panorama des risques évolutif en identifiant les perturbations qui méritent une attention supplémentaire.
- Fournir un éclairage et un point de vue sur les risques émergents associés aux événements perturbateurs.
- Trouver et attirer des candidats dotés des compétences requises pour réagir avec rapidité et fermeté aux risques nouveaux ou émergents.
- Collaborer avec d'autres fonctions de management des risques et de conformité.

Conclusion

Les risques mis en évidence dans le présent rapport, bien que désignés par les instituts affiliés de l'IIA comme des sujets de préoccupation majeurs, ne sont pas les seuls risques auxquels les organisations ou l'audit interne font face. En plus de ces domaines, les instituts affiliés ont également identifié des risques inhérents au comité d'audit, au budget, aux lignes de maîtrise et à la stratégie, soit autant de domaines essentiels à la gouvernance de l'organisation qui doivent

être reconnus et examinés. Les risques peuvent compromettre la mission et les objectifs stratégiques d'une organisation et menacer la valeur globale de celle-ci. De ce fait, la responsabilité de l'audit interne, en tant que conseiller de confiance sur les processus de management des risques, de contrôle et de gouvernance, nécessite de prendre en compte tous les risques potentiels et de formuler des recommandations appropriées.

Dans le monde entier, les organisations s'appuient sur l'audit interne et sur ses évaluations. Pour rester pertinent et être reconnu en tant que conseiller de confiance, l'audit interne a l'obligation de prendre en considération les risques pouvant empêcher la réalisation de ses propres objectifs, ainsi que les objectifs de l'organisation. Pour cette raison, l'audit interne doit être focalisé sur les résultats et déterminé à améliorer ses capacités au profit de l'organisation dans son ensemble. Cela implique la capacité de surmonter les défis et les obstacles, mais aussi de faire preuve d'esprit critique, de rester indépendant, objectif et agile ; de se concentrer sur le *leadership* pour affronter les risques, réels ou supposés, de faire preuve de prospective en fonctionnant comme un consultant en cas de besoin, de fournir une assurance si nécessaire ; et de comprendre l'interdépendance de tous les systèmes, processus, réglementations et opérations.

Instituts affiliés à l'IIA

Les instituts affiliés sont les piliers de l'IIA. L'IIA s'associe aux instituts affiliés dans plus de 170 pays et territoires pour remplir sa mission visant à promouvoir la profession d'audit interne et à servir ses quelque 190 000 répartis dans le monde entier. Représentants exclusifs de l'IIA et porte-parole de la profession, les instituts affiliés contribuent à la diffusion de normes éthiques élevées et de bonnes pratiques dans leurs communautés respectives.

À propos de l'IIA

Porte-parole mondial de la profession d'audit interne, l'*Institute of Internal Auditors* (IIA) est une autorité reconnue et un leader incontesté dans la formation et la formulation de normes, lignes directrices et certifications. Fondé en 1941, l'IIA compte actuellement quelque 190 000 membres dans plus de 170 pays et territoires.
Son siège se situe à Lake Mary (Floride) aux États-Unis. Plus d'informations sont disponibles sur le site www.globaliia.org

Clause de non-responsabilité

Les opinions exprimées dans les Perspectives internationales ne sont pas nécessairement celles des auteurs ayant collaboré à l'élaboration du présent document ni celles des collaborateurs.

Copyright

The Institute of
Internal Auditors

globaliia.org