
2024
RISK IN FOCUS
(LES PRINCIPAUX RISQUES)
Sujets d'actualité
pour les auditeurs
internes
AMÉRIQUE DU NORD
Lire la suite
Internal Audit
FOUNDATION

AU SUJET DU RISK IN FOCUS

Risk in Focus met à la disposition des auditeurs internes et de leurs parties prenantes une recherche pratique axée sur des données afin de les aider à comprendre l'environnement de risque actuel et dresser des plans d'audit pour l'année à venir.

Les rapports reposent sur un sondage mondial pour identifier les risques actuels et émergents pour chaque région, suivi de tables rondes et d'entrevues visant à découvrir des pratiques exemplaires pour les auditeurs internes.

Chacune des six régions de l'IAI recevra deux rapports:

- **Sujets d'actualité pour les auditeurs internes** – Rapports détaillés basés sur les sondages, tables rondes et entrevues.
- **Document d'information pour le Conseil** – Rapports de synthèse que les auditeurs internes doivent partager avec les parties prenantes.

Global Risk in Focus est un partenariat de collaboration facilité par **Internal Audit Foundation** grâce au soutien généreux des organismes régionaux de l'IAI, des Institutes de l'IAI et des sociétés commanditaires. 2024 marque la première année où le projet a été mené à travers le monde.

La méthodologie Risk in Focus a été initialement créée en 2016 par le European Institutes Research Group (EIRG) (le Groupe de recherche des instituts européens), qui continue à la publier en Europe au moyen de la European Confederation of Institutes of Internal Auditing (ECIAI) (la Confédération européenne des Instituts d'audit interne).

Les rapports sont offerts gratuitement au grand public sur la page de ressources Risk in Focus resource page de l'IAI et sur les sites Web pour les groupes régionaux IAI: ACIAI (Asie Pacifique), AFIAI (Afrique), ARABCIAI (Moyen-Orient), ECIAI (Europe), FLAI (Amérique latine).

PROMOTEUR DES RAPPORTS EN AMÉRIQUE DU NORD

AUDITBOARD

TABLE DES MATIÈRES

Table des matières

SOMMAIRE - AMÉRIQUE DU NORD

S'adapter à une évolution rapide par la collaboration

Après une période de trois ans de perturbation mondiale sans précédent, les entreprises nord-américaines sont à la recherche d'une collaboration plus étroite avec les parties prenantes à travers leurs entreprises afin d'aller au-devant d'un paysage des risques en pleine évolution. Les chefs de l'audit interne agissent souvent comme conseillers du conseil d'administration et des dirigeants pour les projets stratégiques et réorganisent les méthodologies d'audit afin de mieux gérer les risques à venir.

Risk in Focus pour l'Amérique du Nord offre un aperçu des questions urgentes auxquelles les CAE et leurs conseils d'administration sont confrontés, notamment:

- Quels sont les principaux risques auxquels les entreprises sont confrontées dans la région? Comment ces risques évolueront-ils au cours des trois prochaines années?
- Où les auditeurs internes investissent-ils le plus de temps et d'efforts?
- Comment les fonctions d'audit internes puissent-elles aider les entreprises?

Deux risques dominent le paysage des risques pour l'Amérique du Nord en 2024 – la cybersécurité et le capital humain, qui transcendent presque chaque aspect des activités d'une entreprise. D'ici 2027, les CAE s'attendent à ce que la cybersécurité soit le risque le plus important, mais la perturbation numérique occupera la deuxième place – pendant que les niveaux de risque augmenteront considérablement en matière de changement climatique.

Selon les répondants au sondage à travers le monde, les trois secteurs à risque élevé sont la cybersécurité, le capital humain et la continuité d'activité. Dans toutes les régions, un remarquable consensus a été atteint en ce qui concerne le fait que la perturbation numérique et le changement climatique sont les deux secteurs où on s'attend le plus à la croissance du niveau de risque et de l'effort d'audit.

Les rapports Risk in Focus en Amérique du Nord décrivent en détail les défis et les solutions pour les secteurs de risque urgents et s'appuient sur l'expertise, l'expérience et les connaissances de nombreux chefs d'audit interne à travers la région. Les thèmes d'intérêt pour les rapports de l'Amérique du Nord sont la cybersécurité, le capital humain, l'évolution du marché et la continuité d'activité.

Pour une synthèse des conclusions à fournir aux conseils d'administration et aux parties prenantes, veuillez consulter North America Risk in Focus 2024 – Board Briefing (Risk in Focus 2024 en Amérique du Nord – Document d'information pour le Conseil). Pour des rapports provenant d'autres régions, veuillez consulter la page de ressources Risk in Focus.

Participation à la recherche en Amérique du Nord

- **442 réponses au sondage** des CAE et administrateurs
- **Pays participants:** Les États-Unis (385), le Canada (57)
- **4 tables rondes** avec 28 participants
- **9 entrevues approfondies**

MÉTHODOLOGIE

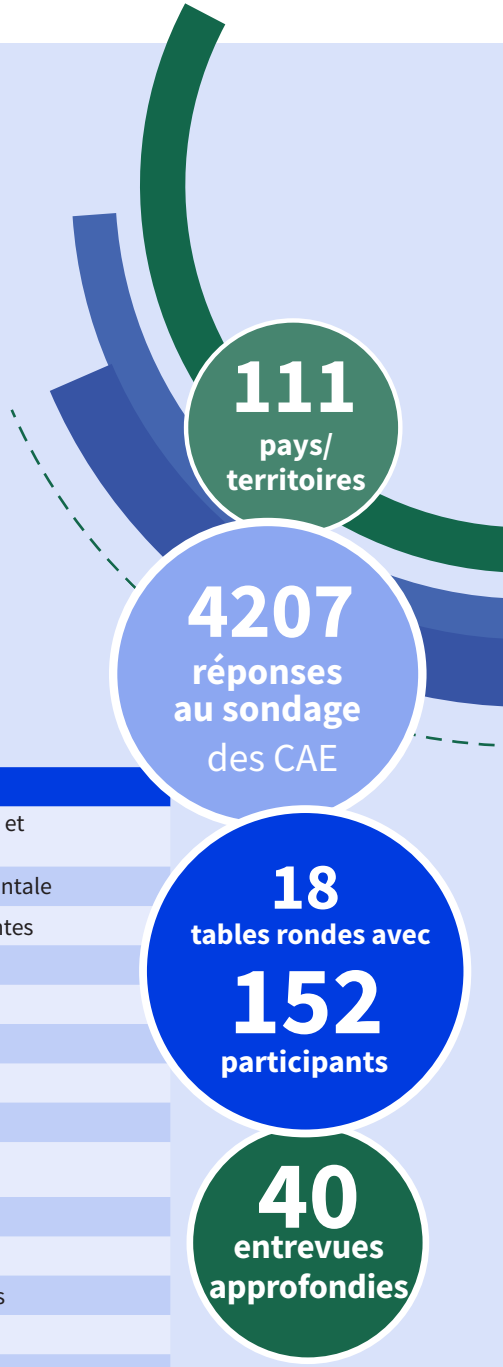
La méthodologie Risk in Focus débute avec un sondage parmi les CAE et les responsables d'audit interne pour identifier les risques actuels et émergents pour chaque région. Les principaux risques identifiés dans le sondage sont utilisés dans des tables rondes de suivi et des entrevues avec les CAE, les universitaires et d'autres spécialistes de l'industrie.

Le sondage présente 16 catégories de risque, telles que mentionnés ci-dessous. Les répondants sont invités à choisir les premières 5 catégories les plus élevées pour le niveau de risque et les premières 5 catégories les plus élevées pour le temps et les efforts consacrés à l'audit interne – aujourd'hui et pour trois années dans l'avenir. Dans les rapports, les catégories sont référencées par leurs noms abrégés.

Pour le projet mondial Risk in Focus 2024, 4 207 CAE et administrateurs provenant de 111 pays / territoires ont répondu au sondage entre le 15 février et le 12 juillet 2023. Dix-huit tables rondes ont été organisées avec 152 participants, suivies par 40 entrevues approfondies.

Catégories de risque Risk in Focus 2024

Thème du risque	Description du risque utilisée dans le sondage
Continuité d'activité	Continuité d'activité, résilience opérationnelle, gestion de crises et intervention en cas de catastrophe
Changement climatique	Changement climatique, biodiversité et durabilité environnementale
Communications/réputation	Communications, réputation et relations avec les parties prenantes
Cybersécurité	Cybersécurité et sécurité des données
Perturbation numérique	Perturbation numérique, nouvelle technologie et IA
Liquidité financière	Risques financiers, de liquidités et d'insolvabilité
Fraude	Fraude, corruption et exploitation criminelle de la perturbation
Incertitude géopolitique	Incertitude macroéconomique et géopolitique
Déclarations de gouvernance / d'entreprise	Déclarations de gouvernance organisationnelle / d'entreprise
Santé et sécurité	Santé, sûreté et sécurité
Capital humain	Capital humain, diversité et gestion et rétention de talents
Évolution du marché	Évolution du marché / concurrence et comportement des clients
Fusions et acquisitions	Fusions et acquisitions
Culture organisationnelle	Culture organisationnelle
Changements réglementaires	Changements législatifs et réglementaires
Chaîne logistique et externalisation	Chaîne logistique, externalisation et risque des parties 'nièmes'



RÉSULTATS DU SONDAGE - AU NIVEAU MONDIAL

Comparaisons régionales

La participation mondiale au sondage Risk in Focus offre une rare occasion de comparer le risque et la planification de l'audit entre les différentes régions.

Comment utiliser les résultats du sondage

Les résultats du sondage Risk in Focus sont présentés dans un ensemble de graphiques illustrant les réponses au sondage sur les niveaux de risque et l'effort d'audit – à présent et pour trois années dans l'avenir. Les principales constatations sont résumées ci-dessous, mais les lecteurs sont encouragés à examiner les graphiques en détail pour plus d'information.

Le premier ensemble de graphiques présente des résultats de haut niveau pour les répondants du monde entier – comparés par région.
La section de graphiques suivante présente des résultats détaillés pour la région prioritaire visé par ce rapport.

Les pourcentages indiquent combien de personnes ont choisi le secteur de l'audit comme l'un des cinq domaines les plus importants pour le niveau de risque ou l'effort d'audit au sein de leur entreprise.

Dans les graphiques, les résultats pour les niveaux de risque sont de couleur bleue et les résultats pour l'effort d'audit sont de couleur verte; les niveaux actuels ont des tons plus foncés et les niveaux futurs ont des tons plus clairs.

Sommaire – Mondial

Figure 1: Les premiers 5 risques les plus élevés par région – Mondial

Il existe un large consensus mondial que les trois secteurs à haut risque pour les entreprises où les CAE déroulent leur travail sont:

1. La cybersécurité
2. Le capital humain
3. La continuité d'activité

Pour la plupart des régions, les changements réglementaires sont classés également entre les premiers 5 risques les plus élevés, à l'exception de l'Afrique et du Moyen-Orient, où les liquidités financières constituent une préoccupation plus importante. En reflétant les événements actuels et les préoccupations futures, l'instabilité géopolitique est en tête de liste pour l'Amérique latine et l'Europe. L'évolution du marché est considérée comme un risque majeur pour l'Asie Pacifique et l'Amérique du Nord, mais pas dans les autres régions.

Sondage mondial – Réponses par région

Afrique	808
Asie Pacifique	1035
Amérique Latine (et Caraïbes)	956
Europe	799
Amérique du Nord	442
Moyen-Orient	167
Total	**4207**

RÉSULTATS DU SONDAGE - MONDIAL

Finalement, l'Afrique était le seul pays ayant la fraude comme l'une de ses premières 5 préoccupations, alors que le Moyen-Orient était le seul ayant les déclarations de gouvernance organisationnelle / d'entreprise dans leurs premières 5 préoccupations.

Une autre façon d'examiner les données est de déterminer quelle région avait le risque le plus élevé dans chaque secteur d'audit. Par exemple, les risques liés au changement climatique étaient classés comme les plus élevés en Europe, par rapport à d'autres régions. Quelques points remarquables sur les classements les plus élevés par secteur d'audit comprennent:

- Les répondants Nord-Américains ont apprécié la cybersécurité (85%) et le capital humain (65%) comme ayant les niveaux de risque les plus élevés par rapport à d'autres régions.
- En Europe, bien que la cybersécurité constitue un risque presque aussi élevé qu'en Amérique du Nord (84%) les autres secteurs de haute préoccupation étaient l'incertitude géopolitique (43%) et le changement climatique (31%). L'Europe a été la seule région où le changement climatique dépasse 30%.
- L'Amérique latine partageait la préoccupation de l'Europe en ce qui concerne l'incertitude géopolitique (42%), en signalant également un haut risque en matière de changements réglementaires (48%) et de perturbation numérique (38%).
- La région Asie Pacifique était particulièrement préoccupée par la continuité d'activité (61%) et l'évolution du marché (47%), par rapport à d'autres régions.
- Le Moyen-Orient avait des niveaux de risque beaucoup plus élevés pour les déclarations de gouvernance / d'entreprise (45%) que d'autres régions et légèrement plus élevés pour les communications / la réputation (28%).
- Finalement, l'Afrique avait un mélange de risques unique qui sont plus élevés que dans d'autres régions, incluant la liquidité financière (47%), la fraude (46%) et la culture organisationnelle (34%).

Figure 2: Les premiers 5 efforts d'audit par région – Mondial

Bien que les niveaux de risque puissent varier d'une région à une autre, les secteurs avec l'effort le plus élevé pour l'audit interne sont très similaires, généralement dans cet ordre:

1. La cybersécurité
2. Les déclarations de gouvernance / d'entreprise
3. La continuité d'activité
4. Les changements réglementaires
5. La liquidité financière
6. La fraude

Bien que les niveaux de risque puissent varier d'une région à une autre, les secteurs avec l'effort le plus élevé pour l'audit interne sont très similaires.

Le principal domaine de divergence était celui des changements réglementaires, où les pourcentages de l'effort d'audit étaient nettement inférieurs pour l'Afrique (35%) et le Moyen-Orient (35%) que pour d'autres régions, où ils sont à 50% ou plus.

D'autres différences spécifiques étaient:

- La région Asie Pacifique avait un pourcentage plus faible pour la liquidité financière (35%) que la moyenne mondiale (45%).
- L'Amérique latine avait un pourcentage plus faible que d'autres régions en ce qui concerne l'effort pour les déclarations de gouvernance / d'entreprise (46% pour l'Amérique latine c. 55% pour la moyenne mondiale).
- L'Amérique du Nord avait un pourcentage beaucoup plus faible que la moyenne mondiale en ce qui concerne l'effort pour combattre la fraude (26% pour l'Amérique du Nord c. 42% pour la moyenne mondiale).

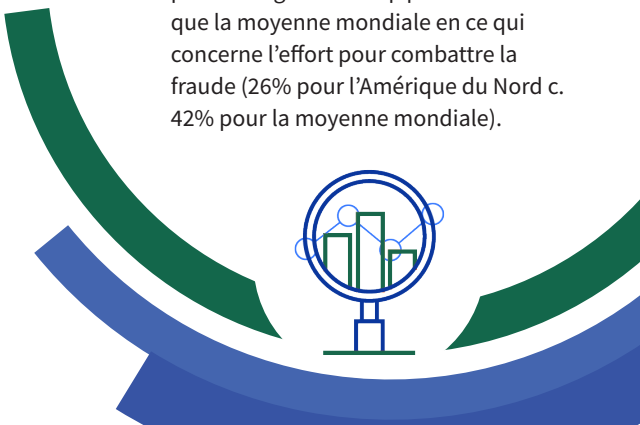


Table des matières

RÉSULTATS DU SONDAGE - MONDIAL

Une autre façon d'examiner les données est de déterminer quelle région avait l'effort d'audit le plus élevé dans chaque secteur d'audit. Dans de nombreux secteurs d'audit, la différence d'effort entre les région est insignifiante. Il existe quand-même certains secteurs d'audit où les différences sont remarquables:

- L'Amérique du Nord était impliqué dans la cybersécurité de manière beaucoup plus large (84%) que d'autres régions, à l'exception de l'Europe (79%).
- L'Afrique a plus d'éléments en ajoutant aux premiers 5 risques les plus élevés l'effort pour combattre la fraude (57%) et la liquidité financière (53%) par rapport à d'autres régions.
- L'Europe a un pourcentage presque double indiquant que le changement climatique représente l'un des premiers 5 risques les plus élevés pour l'effort d'audit (19%) par rapport à la moyenne mondiale (11%).

Figure 3: Prévision sur l'évolution des risques dans trois années – Au niveau mondial

Il existe un consensus mondial que les niveaux de risque augmenteront en matière de perturbation numérique et changement climatique au cours des trois années suivantes. Les deux secteurs ont eu des augmentations de 20 points de pourcentage entre les niveaux de risques actuels et futurs. Plus remarquable encore est la progression dans le classement pour le changement climatique qui a a sauté de la quatorzième à la cinquième position.

Figure 4: Prévision sur l'évolution des efforts d'audit dans trois années – Au niveau mondial

Compte tenu que les niveaux de risque devraient encore augmenter en ce qui concerne la perturbation numérique et le changement climatique, il en va de même pour le temps et l'effort qui devraient être consacrés à l'audit interne dans ces secteurs. Le pourcentage qui s'attend à ce que la perturbation numérique entre dans les premiers 5 pour l'effort d'audit a plus que doublé - de 22% à 52%. Tout aussi remarquable, le pourcentage pour le changement climatique a plus que triplé, de 11% à 34%.

Il existe un consensus mondial que les niveaux de risque augmenteront en matière de perturbation numérique et changement climatique au cours des trois années suivantes.

Figure 1:

Les premiers 5 risques les plus élevés par région – Au niveau mondial

Il existe un large consensus mondial que les trois secteurs à haut risque sont la cybersécurité, le capital humain et la continuité d'activité:

Quels sont les premiers 5 risques auxquels votre entreprise est confrontée actuellement?

Secteur de l'audit	Moyenne de toutes les régions	Asie Pacifique	Amérique latine	Afrique	Amérique du Nord	Moyen-Orient	Europe
Cybersécurité	**73%**	**66%**	**75%**	**58%**	**85%**	**70%**	**84%**
Capital humain	**51%**	**59%**	**44%**	**39%**	**65%**	**47%**	**50%**
Continuité d'activité	**47%**	**61%**	**47%**	**52%**	**36%**	**53%**	**35%**
Changements réglementaires	**39%**	**35%**	**48%**	32%	**43%**	33%	**49%**
Perturbation numérique	**34%**	30%	38%	33%	36%	32%	33%
Liquidité financière	**32%**	21%	33%	**47%**	28%	**38%**	26%
Évolution du marché	**32%**	**47%**	26%	21%	**41%**	26%	30%
Incertitude géopolitique	**30%**	28%	**42%**	25%	28%	16%	**43%**
Déclarations de gouvernance / d'entreprise	**27%**	24%	18%	36%	16%	**45%**	22%
Chaîne logistique et externalisation	**26%**	27%	16%	19%	36%	28%	30%
Culture organisationnelle	**26%**	23%	26%	34%	21%	30%	20%
La fraude	**24%**	22%	30%	**46%**	9%	26%	13%
Communications/réputation	**21%**	18%	22%	27%	21%	28%	12%
Changement climatique	**19%**	22%	22%	19%	12%	10%	31%
Santé et sécurité	**11%**	12%	8%	10%	17%	9%	13%
Fusions et acquisitions	**6%**	4%	3%	3%	8%	10%	8%

Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, n = 4 207. Les pourcentages indiquent qui a classé le secteur comme l'un de leurs premiers 5 secteurs pour le niveau de risque.
La couleur bleu foncé indique les 5 secteurs à haut risque pour la région concernée

Figure 2:

Les premiers 5 efforts d'audit par région – Au niveau mondial

Les secteurs avec l'effort le plus élevé par région

Les secteurs avec l'effort d'audit le plus élevé à travers les régions sont très similaires.

Quels sont les premiers 5 risques auxquels l'audit interne consacre le plus de temps et d'efforts?

Secteur de l'audit	Moyenne de toutes les régions	Asie Pacifique	Amérique latine	Afrique	Amérique du Nord	Moyen-Orient	Europe
Cybersécurité	**68%**	**66%**	**66%**	**54%**	**84%**	**61%**	**79%**
Déclarations de gouvernance / d'entreprise	**55%**	**54%**	46%	**52%**	**55%**	**64%**	**61%**
Continuité d'activité	**54%**	**59%**	**53%**	**56%**	**53%**	**53%**	**50%**
Changements réglementaires	**46%**	**56%**	**50%**	35%	**53%**	35%	**50%**
Liquidité financière	**45%**	35%	**50%**	**53%**	**46%**	**44%**	**45%**
La fraude	**42%**	**42%**	**47%**	**57%**	26%	**43%**	36%
Chaîne logistique et externalisation	**34%**	33%	28%	32%	38%	39%	36%
Capital humain	**30%**	33%	28%	33%	26%	35%	26%
Culture organisationnelle	**24%**	23%	29%	27%	17%	27%	21%
Perturbation numérique	**22%**	19%	24%	24%	25%	20%	21%
Communications/réputation	**20%**	21%	23%	25%	20%	23%	11%
Santé et sécurité	**17%**	18%	12%	13%	21%	16%	19%
Évolution du marché	**16%**	23%	17%	15%	14%	16%	10%
Changement climatique	**11%**	10%	8%	11%	9%	7%	19%
Incertitude géopolitique	**9%**	6%	13%	12%	4%	8%	8%
Fusions et acquisitions	**6%**	3%	5%	2%	10%	8%	9%

Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, n = 4 207. Les pourcentages indiquent qui a classé le secteur comme l'un de leurs premiers 5 secteurs pour le temps et les efforts consacrés à l'audit.
La couleur vert foncé indique les 5 secteurs d'effort d'audit les plus importants pour la région concernée.

Figure 3:

Prévision sur l'évolution des risques dans 3 années – Au niveau mondial

On s'attend à ce que les risques liés au changement climatique augmentent considérablement en passant de la quatorzième à la cinquième position.

Quels sont les premiers 5 risques auxquels votre entreprise est confrontée actuellement?

1.	Cybersécurité	73%
2.	Capital humain	51%
3.	Continuité d'activité	47%
4.	Changements réglementaires	39%
5.	**Perturbation numérique**	**34%**
6.	Liquidité financière	32%
7.	Évolution du marché	32%
8.	Incertitude géopolitique	30%
9.	Déclarations de gouvernance / d'entreprise	27%
10.	Chaîne logistique et externalisation	26%
11.	Culture organisationnelle	26%
12.	Fraude	24%
13.	Communications/réputation	21%
14.	**Changement climatique**	**19%**
15.	Santé et sécurité	11%
16.	Fusions et acquisitions	6%

Quels sont les premiers 5 risques auxquels votre entreprise sera confrontée dans 3 années?

1.	Cybersécurité	67%
2.	**Perturbation numérique**	**55%**
3.	Capital humain	46%
4.	Continuité d'activité	41%
5.	**Changement climatique**	**39%**
6.	Changements réglementaires	39%
7.	Incertitude géopolitique	34%
8.	Évolution du marché	33%
9.	Chaîne logistique et externalisation	25%
10.	Liquidité financière	23%
11.	Culture organisationnelle	21%
12.	Déclarations de gouvernance / d'entreprise	20%
13.	Fraude	20%
14.	Communications/réputation	15%
15.	Santé et sécurité	11%
16.	Fusions et acquisitions	11%

Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, *n* = 4 207. Pourcentage qui a classé le secteur comme l'un des premiers 5 risques les plus élevés de l'entreprise.

Figure 4:

Prévision sur l'évolution des efforts d'audit dans 3 années – Au niveau mondial

Prévision sur le changement des efforts

De fortes augmentations sont attendues pour l'activité d'audit interne liée à la perturbation numérique et au changement climatique.

Quels sont les premiers 5 risques auxquels l'audit interne consacre le plus de temps et d'efforts?

1.	Cybersécurité	68%
2.	Déclarations de gouvernance / d'entreprise	55%
3.	Continuité d'activité	54%
4.	Changements réglementaires	46%
5.	Liquidité financière	45%
6.	Fraude	42%
7.	Chaîne logistique et externalisation	34%
8.	Capital humain	30%
9.	Culture organisationnelle	24%
10.	**Perturbation numérique**	**22%**
11.	Communications/réputation	20%
12.	Santé et sécurité	17%
13.	Évolution du marché	16%
14.	**Changement climatique**	**11%**
15.	Incertitude géopolitique	9%
16.	Fusions et acquisitions	6%

Quels sont les premiers 5 risques auxquels vous prévoyez que l'audit interne va consacrer le plus de temps et d'efforts dans 3 années?

1.	Cybersécurité	73%
2.	**Perturbation numérique**	**52%**
3.	Continuité d'activité	49%
4.	Changements réglementaires	37%
5.	Déclarations de gouvernance / d'entreprise	36%
6.	Capital humain	35%
7.	**Changement climatique**	**34%**
8.	Fraude	29%
9.	Liquidité financière	28%
10.	Chaîne logistique et externalisation	28%
11.	Culture organisationnelle	24%
12.	Évolution du marché	22%
13.	Communications/réputation	16%
14.	Incertitude géopolitique	16%
15.	Santé et sécurité	15%
16.	Fusions et acquisitions	8%

Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, *n* = 4 207. Pourcentage qui a classé le secteur comme l'un des premiers 5 risques les plus élevés de l'entreprise.

RÉSULTATS DU SONDAGE - AMÉRIQUE DU NORD

Comment utiliser les résultats du sondage

Les principales constatations pour l'Amérique du Nord sont résumées ci-dessous, mais les lecteurs sont encouragés à examiner les graphiques suivants en détail pour plus d'information. Les pourcentages indiquent combien de personnes ont choisi le secteur de l'audit comme l'un des cinq domaines les plus importants pour le niveau de risque ou l'effort d'audit au sein de leur entreprise. Les résultats pour les niveaux de risque sont de couleur bleue et les résultats pour l'effort d'audit sont de couleur verte; les niveaux actuels ont des tons plus foncés et les niveaux futurs ont des tons plus clairs.

Figure 5: Les niveaux des risques actuels c. les niveaux des risques futurs - Amérique du Nord

- La cybersécurité et le capital humain ont dominé le paysage des risques en Amérique du Nord pour l'année 2024.
- Dans les 3 prochaines années, la perturbation numérique et le changement climatique sont les risques qui devraient enregistrer la plus haute augmentation.

Figure 6: Prévision sur l'évolution des risques dans 3 années – Amérique du Nord

- On s'attend à ce que la perturbation numérique passe du sixième risque le plus élevé au deuxième risque le plus élevé dans les prochaines 3 années.
- Les risques liés au changement climatique passe des trois dernières positions à la neuvième position.

Figure 7: Les efforts d'audit actuels c. les efforts d'audit futurs - Amérique du Nord

- À majorité écrasante, les CAE ont choisi la cybersécurité comme l'un des premiers 5 secteurs pour l'effort d'audit interne (84%).
- La deuxième place est occupée par les déclarations de gouvernance / d'entreprise, mais on s'attend à ce que ce secteur baisse à l'avenir.

Figure 8: Prévision sur l'évolution des efforts d'audit dans 3 années – Amérique du Nord

- De fortes augmentations sont attendues pour l'activité d'audit interne liée à la perturbation numérique et au changement climatique.
- Les augmentations sont compensées par des baisses pour la liquidité financière et les déclarations de gouvernance / d'entreprise.

Figure 9: Les niveaux des risques actuels c. les efforts d'audit futurs - Amérique du Nord

- Les déclarations de gouvernance / d'entreprise représente un faible risque pour les entreprises (16%), mais un grand effort (55%) pour l'audit interne en Amérique du Nord.

Réponses au sondage par pays en Amérique du Nord

États-Unis	385
Canada	57
Total	**442**

- L'effort est faible par rapport au risque lié à l'incertitude géopolitique, l'évolution du marché et le changement climatique, mais ces risques peuvent être atténués par la liquidité financière, la continuité d'activité ou la chaîne d'approvisionnement.

Figure 10: Les niveaux des risques futurs c. les efforts d'audit futurs - Amérique du Nord

- On s'attend à ce que les niveaux de risque et les efforts soient étroitement alignés dans les 3 prochaines années pour les secteurs de risque croissant de la perturbation numérique (56% /53%) et du changement climatique (30%/27%).

RÉSULTATS DU SONDAGE - AMÉRIQUE DU NORD

Comprendre l'impact de SOX en Amérique du Nord sur les résultats du sondage

Afin de mieux comprendre les activités d'audit en Amérique du Nord, il est important de reconnaître l'effet des exigences Sarbanes-Oxley (SOX) et de la responsabilité au titre de l'ERM (GGR - la gestion globale des risques) sur les fonctions d'audit interne, dit Richard Chambers, Conseiller d'audit principal chez AuditBoard.

La Sarbanes-Oxley Act of 2002 (la loi américaine Sarbanes-Oxley de 2002) a établi d'importantes exigences réglementaires sur les contrôles internes des déclarations financières pour les entreprises cotées en bourse aux États-Unis. L'audit interne est souvent appelé à s'occuper de la part du lion afférente à cet effort, avec 67% des fonctions d'audit interne des entreprises cotées en bourse disant qu'ils ont une responsabilité directe, selon le sondage 2023 North American Pulse of Internal Audit de l'IAI.[1]

Dans le sondage Risk in Focus, l'activité liée à la loi Sarbanes-Oxley relève de la catégorie des déclarations de gouvernance / d'entreprise. Ce secteur figurait au bas du classement en ce qui concerne les risques (16% comme l'un de leurs premiers 5), mais il s'est classé le deuxième en ce qui concerne le temps et les efforts consacrés à l'audit (55% dans les premiers 5). Cet effort vers les déclarations d'entreprise a tendance à éloigner le temps consacré à l'audit des autres secteurs, tout en augmentant les lacunes entre les risques et les efforts dans d'autres secteurs.

En plus du défi en matière de bande passante, Chambers observait que la loi Sarbanes-Oxley peut créer également un défi en matière d'indépendance pour l'audit interne. Parmi les répondants au sondage 2023 Pulse, 72% des CAE des entreprises cotées en bourse disent qu'ils relèvent sur le plan administratif du directeur financier (CFO), qui est souvent responsable du programme SOX.

Cet haut niveau de responsabilité pour le programme SOX, combiné avec le fait de relever sur le plan administratif du CFO, crée un risque que les CAE donnent non seulement des assurances pour les contrôles internes sur les déclarations financières, mais qu'ils assument également, de manière directe, les responsabilités de conformité du CFO. Il s'agit de l'audit interne qui a une indépendance suffisante pour donner des assurances pour les contrôles internes sur les déclarations financière, compte tenu de leurs responsabilités et du rattachement hiérarchique.

Finalement, presque la moitié des CAE des entreprises cotées en bourse (46%) sont également responsables pour l'ERM (la GGR - gestion globale des risques), selon les répondants au sondage 2023 Pulse. Sur le côté positif, lorsqu'un seul rôle est responsable des deux, il pourrait y avoir une meilleure harmonisation entre l'évaluation des risques et l'activité d'audit. Cependant, il importe que les CAE bénéficient d'une formation adéquate sur la méthodologie ERM qui accorde une importance égale aux opportunités et au risque. Finalement, si l'audit interne est responsable de l'ERM, il est préférable qu'un tiers donne des assurances pour l'éfficacité générale de la gestion des risques, parce que la fonction d'audit interne ne devrait pas vérifier sa propre activité.

Lecture recommandée

Le Three Lines Model (le modèle à trois axes) de l'IAI

Risk in Focus se rapporte souvent au Three Lines Model influent, qui explique les rôles de la première, la deuxième et la troisième axe.

Le pouls nord-américain de l'IAI en matière d'audit interne

Ce rapport annuel fournit des repères sur les budgets, le personnel et les responsabilités des CAE.

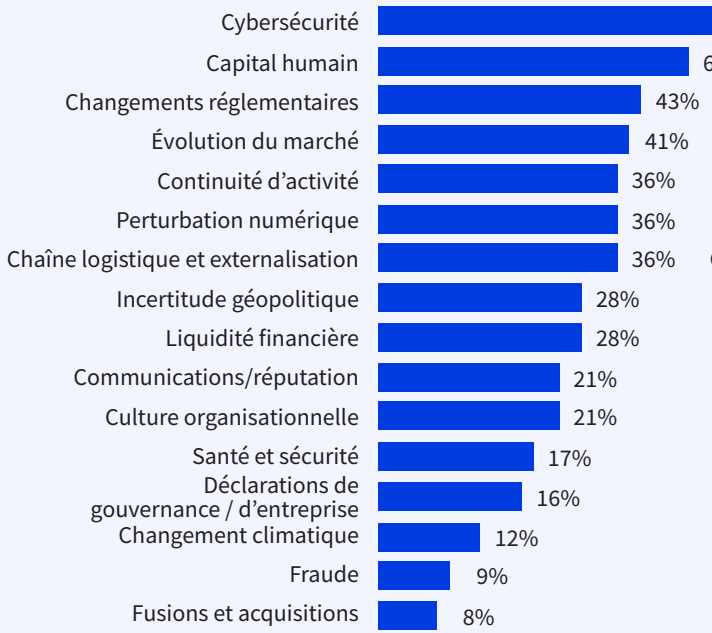
[1] Pour les résultats du sondage cités du Pulse of Internal Audit, veuillez consulter la page 43 (rapports hiérarchiques) et la page 35 (responsabilité pour l'ERM) sur https://www.theiia.org/en/resources/research-and-reports/pulse/

Figure 5:

Les niveaux des risques actuels c. les niveaux des risques futurs - Amérique du Nord

- La cybersécurité et le capital humain ont dominé le paysage des risques en Amérique du Nord pour l'année 2024.
- Dans les 3 prochaines années, la perturbation numérique et le changement climatique sont les risques qui devraient enregistrer la plus haute augmentation.

Quels sont les premiers 5 risques auxquels votre entreprise est confrontée actuellement?



Quels sont les premiers 5 risques auxquels votre entreprise sera confrontée dans 3 années?

Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, Amérique du Nord, *n* = 442. Pourcentage qui a classé le secteur comme l'un des premiers 5 de l'entreprise.

Figure 6:

Prévision sur l'évolution des efforts d'audit dans 3 années – Amérique du Nord

- On s'attend à ce que la perturbation numérique passe du sixième risque le plus élevé au deuxième risque le plus élevé dans les prochaines 3 années.
- Les risques liés au changement climatique passe des trois dernières positions à la neuvième position.

Quels sont les premiers 5 risques auxquels votre entreprise est confrontée actuellement?

1.	Cybersécurité	85%
2.	Capital humain	65%
3.	Changements réglementaires	43%
4.	Évolution du marché	41%
5.	Continuité d'activité	36%
6.	**Perturbation numérique**	**36%**
7.	Chaîne logistique et externalisation	36%
8.	Incertitude géopolitique	28%
9.	Liquidité financière	28%
10.	Communications/réputation	21%
11.	Culture organisationnelle	21%
12.	Santé et sécurité	17%
13.	Déclarations de gouvernance / d'entreprise	16%
14.	**Changement climatique**	**12%**
15.	Fraude	9%
16.	Fusions et acquisitions	6%

Quels sont les premiers 5 risques auxquels votre entreprise sera confrontée dans 3 années?

1.	Cybersécurité	73%
2.	**Perturbation numérique**	**56%**
3.	Capital humain	51%
4.	Changements réglementaires	50%
5.	Évolution du marché	38%
6.	Continuité d'activité	35%
7.	Chaîne logistique et externalisation	31%
8.	Incertitude géopolitique	30%
9.	**Changement climatique**	**30%**
10.	Culture organisationnelle	21%
11.	Liquidité financière	20%
12.	Déclarations de gouvernance / d'entreprise	18%
13.	Communications/réputation	13%
14.	Santé et sécurité	12%
15.	Fusions et acquisitions	12%
16.	Fraude	10%

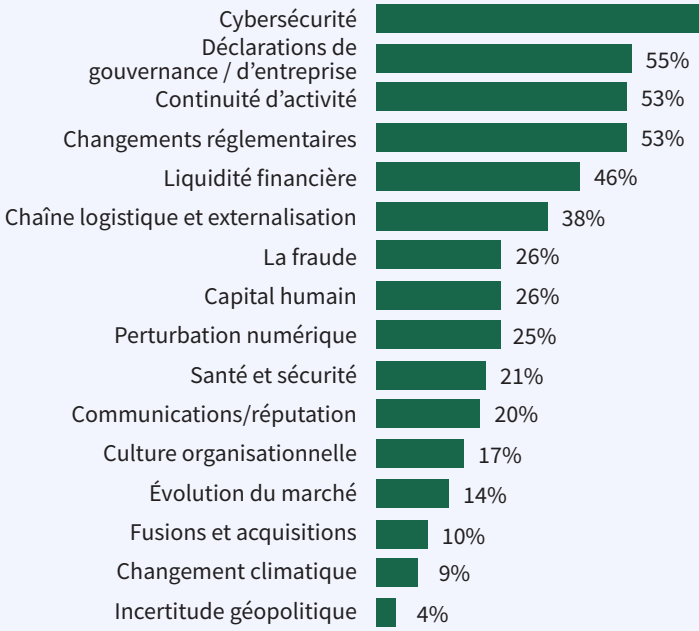
Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, Amérique du Nord, *n* = 442. Pourcentage qui a classé le secteur comme l'un des premiers 5 de l'entreprise.

Figure 7:

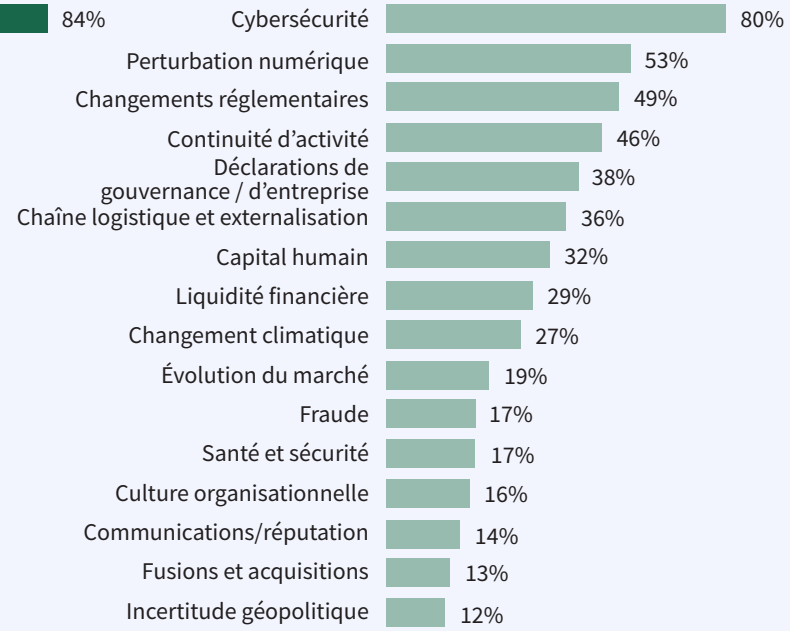
Les efforts d'audit actuels c. les efforts d'audit futurs - Amérique du Nord

- La cybersécurité et le capital humain ont dominé le paysage des risques en Amérique du Nord pour l'année 2024.
- Dans les 3 prochaines années, la perturbation numérique et le changement climatique sont les risques qui devraient enregistrer la plus haute augmentation.

Quels sont les premiers 5 risques auxquels l'audit consacre le plus de temps et d'efforts?



Quels sont les premiers 5 risques auxquels vous prévoyez que l'audit interne va consacrer le plus de temps et d'efforts dans 3 années?



Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, Amérique du Nord, *n* = 442. Le pourcentage qui a classé le secteur comme l'un de leurs premiers 5 secteurs pour le temps et les efforts consacrés à l'audit.

Figure 8:

Prévision sur l'évolution des efforts d'audit dans 3 années – Amérique du Nord

Prévision sur le changement des risques

- De fortes augmentations sont attendues pour l'activité d'audit interne liée à la perturbation numérique et au changement climatique.
- Les augmentations sont compensées par des baisses pour la liquidité financière et les déclarations de gouvernance / d'entreprise.

Quels sont les premiers 5 risques auxquels l'audit interne consacre le plus de temps et d'efforts?

1.	Cybersécurité	84%
2.	Déclarations de gouvernance / d'entreprise	55%
3.	Continuité d'activité	53%
4.	Changements réglementaires	53%
5.	Liquidité financière	46%
6.	Chaîne logistique et externalisation	38%
7.	Fraude	26%
8.	Capital humain	26%
9.	**Perturbation numérique**	**25%**
10.	Santé et sécurité	21%
11.	Communications/réputation	20%
12.	Culture organisationnelle	17%
13.	Évolution du marché	14%
14.	Fusions et acquisitions	10%
15.	**Changement climatique**	**9%**
16.	Incertitude géopolitique	4%

Quels sont les premiers 5 risques auxquels vous prévoyez que l'audit interne va consacrer le plus de temps et d'efforts dans 3 années?

1.	Cybersécurité	80%
2.	**Perturbation numérique**	**53%**
3.	Changements réglementaires	49%
4.	Continuité d'activité	46%
5.	Déclarations de gouvernance / d'entreprise	38%
6.	Chaîne logistique et externalisation	36%
7.	Capital humain	32%
8.	Liquidité financière	29%
9.	**Changement climatique**	**27%**
10.	Évolution du marché	19%
11.	Fraude	17%
12.	Santé et sécurité	17%
13.	Culture organisationnelle	16%
14.	Communications/réputation	14%
15.	Fusions et acquisitions	13%
16.	Incertitude géopolitique	12%

Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, Amérique du Nord, *n* = 442. Le pourcentage qui a classé le secteur comme l'un de leurs premiers 5 secteurs pour le temps et les efforts consacrés à l'audit.

Figure 9:

Les niveaux des risques actuels c. les efforts d'audit futurs - Amérique du Nord

- Le risque est faible pour les déclarations de gouvernance / d'entreprise (16%) mais il est élevé pour l'effort d'audit (55%).
- L'effort n'est pas prioritaire par rapport au risque lié à l'incertitude géopolitique, l'évolution du marché et le changement climatique, mais ces risques peuvent être atténués par la liquidité financière, la continuité d'activité ou la chaîne d'approvisionnement.

Quels sont les premiers 5 risques auxquels votre entreprise est confrontée actuellement?

Quels sont les premiers 5 risques auxquels l'audit interne consacre le plus de temps et d'efforts?

Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, Amérique du Nord, *n* = 442. Le pourcentage qui a classé le secteur comme l'un de leurs premiers 5 secteurs pour le risque ou l'effort d'audit interne.

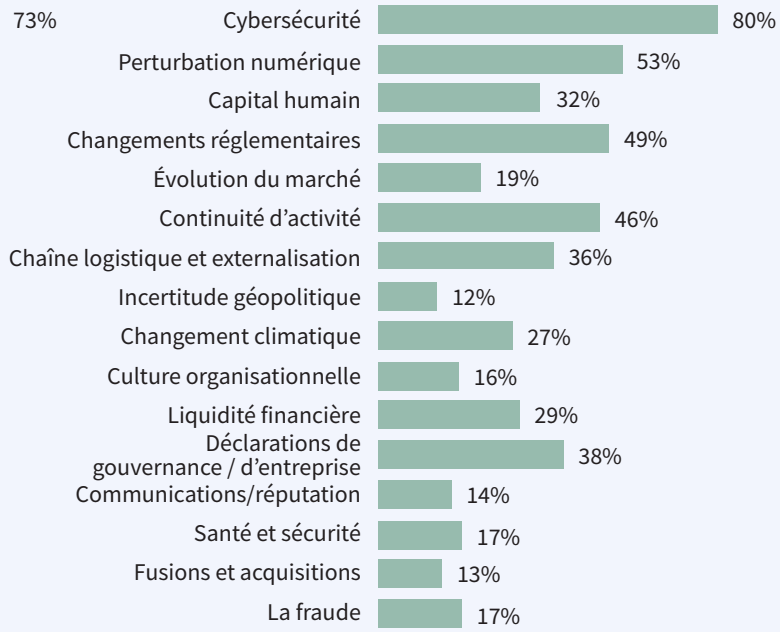
Figure 10:

Les niveaux des risques futurs c. les efforts d'audit futurs - Amérique du Nord

On s'attend à ce que les niveaux de risque et les efforts soient étroitement alignés dans les 3 prochaines années pour les secteurs de risque croissant de la perturbation numérique (56% à 53%) et du changement climatique (30% à 27%).

Quels sont les premiers 5 risques auxquels votre entreprise sera confrontée dans 3 années?

Quels sont les premiers 5 risques auxquels vous prévoyez que l'audit interne va consacrer le plus de temps et d'efforts dans 3 années?



Note: Risk in Focus Global Survey (l'enquête mondiale des principaux risques) de l'IAI, Amérique du Nord, *n* = 442. Le pourcentage qui a classé le secteur comme l'un de leurs premiers 5 secteurs pour le risque ou l'effort d'audit interne.

CYBERSÉCURITÉ

Développement de l'esprit d'équipe pour la cyberrésilience

Parce que la plupart des entreprises s'attendent à être piratées, elles se concentrent sur le renforcement de la résiliation par une collaboration à l'échelle de toute l'entreprise et par une formation continue.

La pandémie a obligé de nombreuses entreprises à déployer leurs systèmes d'information rapidement, souvent en utilisant des fournisseurs tiers de services infonuagiques, afin de permettre aux membres du personnel de travailler de chez eux pendant les confinements. En conséquence, le piratage informatique s'est intensifié et industrialisé juste au moment ou les vastes réseaux étaient les plus vulnérables. Non seulement le risque de cyberattaques soutenues par les États ont augmenté en raison de l'incertitude géopolitique – notamment la guerre en Ukraine et les tensions entre les États-Unis et la Chine – mais l'industrie florissante des cyberattaques en tant que service signifie que les pirates informatiques amateurs pourraient effectuer des escroqueries sophistiquées pour une fraction du temps et du coût.[2]

Ces tendances ont augmenté tant les impacts financiers potentiels des atteintes réussies que le risque de menaces existentielles de la part des soi-disantes attaques de type wiper: les experts craignent que ces coups de type knock-out ciblant actuellement les réseaux ukrainiennes pourraient se propager aux États-Unis.[3] Le coût moyen d'une fuite de données en Amérique du Nord a augmenté de 12,7% en 2020 à 4,35 million de dollars en 2022, selon IBM. Et 83% des répondants ont déclaré qu'ils ont été victimes de multiples fuites, avec 45% de celles-ci se produisant dans le nuage.[4]

Résultats du sondage – cybersécurité

1ER – NIVEAU DE RISQUE

85% l'ont classée dans les premiers 5 *pour le niveau de risque*

1ER – EFFORT D'AUDIT

84% l'ont classée dans les premiers 5 *pour l'effort d'audit*

[2] Pour plus de détails sur les cyberattaques en tant que service, veuillez vous rendre sur https://fieldeffect.com/blog/cybercrime-as-a-service
[3] Pour plus de détails sur les logiciels malveillants de type wiper, veuillez vous rendre sur https://techcrunch.com/2022/02/28/fbi-cisa-ukraine-wiper-malware/
[4] Pour plus de détails sur le coût des fuites de données, veuillez vous rendre sur https://www.ibm.com/downloads/cas/3R8N1DZJ

CYBERSÉCURITÉ

La nouvelle règle de la SEC ajoute de la structure

En juillet 2023, la U.S. Securities and Exchange Commission (SEC) (la Commission des opérations de bourse des États-Unis) a adopté de nouvelles règles pour le signalement d'incidents et la divulgation d'activités ayant trait à la gestion des risques de cybersécurité, à la stratégie et à la gouvernance. L'un de ses objectifs est d'améliorer la cohérence de l'information et de la rendre plus facile à utiliser pour les décideurs et les investisseurs.[5]

Les règles de la SEC reposent sur un enchevêtrement existant de réglementations sur la cybersécurité. Aux États-Unis, il y avait plus de 250 projets de loi ou résolutions proposés au niveau d'État ou au niveau fédéral en 2021.[6] Pour ceux applicables à travers plusieurs juridictions, le temps nécessaires pour suivre leur évolution peut être considérable, dit un CAE d'une société internationale de services financiers. Elle décrit les efforts considérables déployés pour se tenir au courant des exigences, comme l'utilisation de services des consultants en matière de cybersécurité jusqu'à la communication régulière avec les membres de la communauté juridique, le Ministère de la Justice et d'autres CAE afin de s'assurer que l'entreprise est en pleine conformité.

La cyberdéfense exige des connaissances

Le degré de sensibilisation aux cyberattaques est élevé parmi les membres des conseils d'administration et de la direction générale, mais il en va de même pour la pénurie de talents en matière de compétences informatiques et cybernétiques clés, disent les CAE présents à la table ronde. Les postes sont difficiles à pourvoir. Il n'est pas étonnant que le capital humain ait été classé le deuxième risque le plus élevé, avec 65% des répondants au sondage qui l'ont évalué comme l'un des premiers 5 en termes de niveau de risque (voir la Figure 1). Les CAE de petites entreprises et du secteur public déclarent que le manque de personnel est particulièrement grave pour eux, parce qu'il est difficile d'offrir des rémunérations ou des perspectives professionnelles aussi élevées que dans les grandes entreprises et le secteur privé.

Le déficit de talents est moins bien mis en valeur dans les salles des conseils d'administration. Plusieurs CAE présents à la table ronde ont convenu qu'en absence des connaissances informatiques et cybernétiques spécialisées du comité d'audit ou du conseil d'administration, les recommandations peuvent tomber dans des oreilles de sourds. « Jusqu'à ce qu'on trouve quelqu'un pour ce poste de surveillance, qui comprend véritablement ce qu'un programme doit inclure en matière de cybersécurité et de protection des données, qui comprend les recommandations du responsable de la sécurité et de l'audit interne, vous n'aurez aucun progrès important au sein de l'entreprise », dit un CAE d'une société énergétique nord-américaine cotée en bourse .

Ressources

Évaluation du risque de cybersécurité: Le Three Lines Model (le modèle à trois axes)

Vérification de la réponse aux incidents cybernétiques ou du rétablissement

Vérification des opérations de cybersécurité: Prévention et détection

[5] Pour plus de détails sur les nouvelles règles de la SEC, veuillez vous rendre sur https://www.sec.gov/news/press-release/2023-139
[6] Pour plus de détails sur la législation en matière de cybersécurité aux États-Unis, veuillez vous rendre sur https://www.ncsl.org/technology-and-communication/cybersécurité-legislation-2021

CYBERSÉCURITÉ

Certaines entreprises de premier plan élèvent le poste d'officier principal de la sécurité de l'information (OPSI) dans le cadre de la structure de gouvernance de sorte qu'il soit plus facile de mettre en commun les connaissances, de partager les recommandations et de soulever des problèmes. « Si l'OPSI estime qu'il existe une exposition et le dirigeant principal de l'information refuse de s'en occuper, il est essentiel qu'il ou elle ait l'indépendance d'aller directement au CAE ou au comité d'audit pour se faire entendre », dit Karen Percent, CAE dans le secteur des soins de santé.

La plupart des CAE présents à la table ronde ont déclaré avoir renforcé la formation et la sensibilisation afin de lutter contre les développements continus des logiciels malveillants et les attaques par piratage psychologique. Ils amènent tout le monde, du PDG au personnel débutant, à participer à des exercices de faux attaques par hameçonnage qui incorporent des méthodologies de hameçonnage récentes, avec un effort supplémentaire là où on identifie des faiblesses. Le fait de donner le ton au somment et de le faire d'une manière visible fait la différence.

Les entreprises simulent des scénarios élaborés de piratage, défense et rétablissement pour s'assurer que l'équipe de direction et le conseil d'administration sont prêts à prendre des décisions stratégiques si un attaque par rançongiciel se produit. Ceci est combiné avec l'utilisation des services fournis par des pirates informatiques éthiques pour tester les contrôles en ligne et de défense opérationnelle.

> « La création de partenariats solides et de confiance est à la base de tout ce que nous faisons – il est essentiel d'être flexible, agile ainsi que d'être à l'écoute de vos partenaires commerciaux et de collaborer avec eux. »

« Vous allez être piraté – cela va se passer », dit un universitaire d'une école de commerce américaine de premier plan », donc l'objectif clé actuel du conseil d'administration est de détecter et corriger. »

La collaboration est la clé du succès

Plus important encore, la collaboration à travers l'entreprise est essentielle. Les problèmes liés à la cybersécurité et à la sécurité des données ne se trouvent pas dans une seule partie d'une entreprise; ils sont omniprésents. Cela signifie que les risques, les contrôles et les mesures d'atténuation impactent également de multiples fonctions de l'entreprise. Ada Leung, Vice-présidente et CAE chez Fidelity au Canada, dit que l'adoption d'un modèle d'assurance intégré[7] a aidé sont département d'audit interne à identifier et à se concentrer sur les secteurs à haut risque. En outre, la migration vers une plateforme technologique à l'échelle de l'entreprise signifiait que l'entreprise pouvait utiliser une seule taxonomie des risques – un seul langage – à travers ses trois axes pour la technologie de l'information – un autre avantage.

« Tout comme une entreprise ne peut pas dérouler ses activités de manière cloisonnée avec succès, l'audit interne non plus », dit-elle. « La création de partenariats solides et de confiance est à la base de tout ce que nous faisons – il est essentiel d'être flexible, agile ainsi que d'être à l'écoute de vos partenaires commerciaux et de collaborer avec eux. »

[7] Pour plus de détails sur l'audit intégré, veuillez vous rendre sur https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/practice-guide-integrated-approaches-to-internal-auditing/

Table des matières

Sommaire

CYBERSÉCURITÉ

Cela comprend également le fait d'être à l'écoute du personnel et de faire attention aux points faibles potentiels. Les routines qui rend les tâches quotidiennes des gens difficiles, comme les réseaux virtuels maladroits, peuvent être contournées en créant des points d'éclair pour le contrôle des risques cybernétiques. La direction peut essayer de mettre en œuvre des solutions en dehors de tout contrôle informatique, en créant une « TI dans l'ombre » qui est prête au piratage. Une solution est de centraliser les processus de gouvernance pour la cybersécurité dans les départements informatiques et loin de la direction de sorte que les départements informatiques disposent d'une visibilité complète sur toute utilisation de la technologie.

Les CAE présents à la table ronde dit que les principales missions d'audit interne comprenaient:

- Rassembler les inventaires de la gestion d'actifs informatiques de sorte que les programmes de correction couvrent l'entière entreprise.
- Évaluer la maturité de l'entière entreprise en termes de cybersécurité afin de créer une analyse des lacunes sur l'environnement des contrôles.
- Vérifier la gestion des risques à l'échelle de l'entreprise afin de tester son exhaustivité et efficacité en termes de cybersécurité.
- Collaborer avec les départements d'informatique et de gestion des risques afin de créer des contrôles continus pour la surveillance de la cyberdéfense ainsi que des contrôles opérationnels.

Dans trois ans, les répondants aux sondage s'attendent à ce que la cybersécurité soit toujours l'un des premiers éléments de la liste en termes de niveaux de risque et d'efforts d'audit. Avec les progrès technologiques, comme l'intelligence artificielle, en plein essor pendant cette période, et les tensions entre les États-Unis et la Chine au sujet du Taiwan, le paysage des risques devrait devenir toujours plus complexe – et potentiellement plus dangereux.

La direction peut essayer de mettre en œuvre des solutions en dehors de tout contrôle informatique, en créant une « TI dans l'ombre » qui est prête au piratage

CYBERSÉCURITÉ

Comment l'audit interne peut aider l'entreprise

1. Évaluez le niveau de sensibilisation, connaissances et compétences des parties clés de l'entreprise, y compris celles du conseil d'administration, afin de vous assurer que les réponses en matière de cyberdéfense sont pertinentes et à jour.
2. Évaluez les rapports hiérarchiques entre l'OPSI (Officier principal de la sécurité de l'information), le DPI (Dirigeant principal de l'information) et le conseils d'administration afin de vous assurer que les risques et les recommandations sont clairement communiqués et peuvent être renvoyés au plus haut niveau, si nécessaire.
3. Évaluez la fréquence, l'actualité et l'efficacité des exercices de faux attaques par hameçonnage et d'autres activités de sensibilisation ainsi que les niveaux d'engagement de la part du personnel et leur intégration adéquate en matière de formation et de processus de suivi.
4. Utilisez des scénarios de simulation tant pour sensibiliser les membres du conseil d'administration à leurs responsabilités de gouvernance que pour tester l'exhaustivité et l'efficacité des processus d'atténuation.
5. Évaluez l'efficacité du milieu des contrôles et la mesure dans laquelle les contrôles sont intégrés dans la première et la seconde axe, tout en prêtant une attention particulière aux pratiques considérées par les membres du personnel comme étant perturbatrices ou intrusives et qu'ils/elles sont susceptibles d'ignorer, oublier ou contourner.
6. Évaluez les processus de gouvernance autour de la TI dans l'ombre et si la deuxième et la seconde axe peuvent utiliser ces technologies et les contrôles s'y rapportant.
7. Évaluez la mesure dans laquelle la structure de gouvernance de l'entreprise permet la collaboration à travers les trois axes.
8. Évaluez la mesure dans laquelle l'entreprise se tient au courant de l'évolution mondiale des réglementations en matière de cybersécurité et technologie et la facilité avec laquelle les contrôles des données peuvent être changés afin de répondre aux exigences futures.

Table des matières

Sommaire

CAPITAL HUMAIN

Repenser la culture d'entreprise

Dans une économie de graves pénuries de compétences et talents, les CAE aident les entreprises à diversifier leurs pratiques de travail ainsi que leurs stratégies de recrutement et rétention du personnel.

Le risque lié au capital humain transcende chaque secteur stratégique et opérationnel des entreprises. Les entreprises ne peuvent pas fonctionner efficacement sans des gens avec des compétences appropriées – que ce soit pour atteindre leurs objectifs ou pour identifier, gérer et atténuer les risques clés. En raison des tendances, telles que la numérisation, et des risques émergents complexes, tels que le changement climatique, les entreprises doivent avoir une gamme d'expertise plus large et plus profonde à travers un plus ample éventail de secteurs. Mais elles sont confrontées à des déficits majeurs en compétences fondamentales. En cybersécurité, une étude a estimé un nombre de 750 000 de postes non pourvus aux États-Unis.[8]

Accélérés par la pandémie, les changements à la culture du travail ont durement frappé en Amérique du Nord. La soi-disante Grande Résignation – un processus qui a vu des millions de travailleurs qualifiés et expérimentés ayant quitté leurs postes, car les confinements ont déclenché une réévaluation des priorités personnelles – continue. Environ 4 millions de personnes (2,6% de la main d'œuvre des États-Unis) ont quitté leurs postes en octobre 2022 seulement.[9] De plus, de nombreux jeunes ont cessé d'apprécier les valeurs traditionnelles et la culture du travail d'entreprise. Non seulement la plupart d'entre eux insistent sur des pratiques d'emploi flexibles – notamment le travail hybride – main un nombre croissant d'entre eux apprécient faire partie d'entreprises engagées.[10]

Résultats du sondage – Capital humain

2ÈME – NIVEAU DE RISQUE

65% l'ont classée dans les premiers 5 *pour le niveau de risque*

8ÈME – EFFORT D'AUDIT

26% l'ont classée dans les premiers 5 *pour l'effort d'audit*

[8] Pour plus de détails sur les pénuries de personnel cybernétique, veuillez vous rendre sur https://www.esentire.com/resources/library/2023-official-cybersecurity-jobs-report

[9] Pour plus de détails sur la Grande Résignation, veuillez vous rendre sur https://www.weforum.org/agenda/2023/01/us-workers-jobs-quit/

[10] Pour plus de détails sur le travail hybride, veuillez vous rendre sur https://www.mckinsey.com/~/media/mckinsey/email/genz/2022/05/17/2022-05-17b.html / Pour plus de détails sur les valeurs du travail, veuillez vous rendre sur https://time.com/6176169/what-young-workers-want-in-jobs/

CAPITAL HUMAIN

Les CAE présents à la table ronde ont convenu que la création d'une réponse organisationnelle flexible et disposant de ressources suffisantes constitue une priorité absolue des conseils d'administration. Mais ceci a été rendu plus difficile en raison de la nécessité de réduire les coûts et de lutter contre les demandes d'augmentation des salaires dans un environnement atteint par des pressions inflationnistes. En même temps, les membres du personnel demandent aux employeurs de renforcer leurs politiques en matière de diversité, équité et inclusion (DEI) en milieu de travail. Cela a vu un nombre croissant d'entreprises mettant en œuvre volontairement des codes démontrant qu'elles prennent la transformation culturelle au sérieux. En février 2023, plus de 100 entreprises du secteur des finances à travers les États-Unis et le Canada ont adopté le Code DEI volontaire spécifique à l'industrie.[11]

Les cadres moyens donnent le ton pour le travail hybride

Mais pas tous les cadres supérieurs sont d'accord avec les tendance de travail hybride. « Il existe des membres du conseil d'administration qui se demandent pourquoi nous pratiquons toujours le travail hybride lorsque tout le monde semble revenir au bureau » dit un CAE du secteur public américain. « Mais le travail hybride est une [option] clé pour nous, parce qu'il nous aide à attirer et retenir des talents. »

L'adoption de styles de travail hybride est une stratégie populaire – mais elle présente quand-même certains risques. Premièrement, sans participer à des événements en milieu de travail en temps réel et en personne, il y a moins de possibilités d'encadrer et de former le personnel jeune, dit le CAE d'une société de services professionnels en Amérique du Nord. En conséquence, cela prend plus de temps à ses employés pour assimiler les valeurs et la culture de l'entreprise, surtout dans les entreprises plus décentralisées. Deuxièmement, les compétences non techniques fondamentales des employés récemment diplômés pourraient être moins développées – beaucoup d'entre eux ayant terminé leurs années universitaires devant des écrans d'ordinateur parce que l'enseignement supérieur a été mis en confinement. Il est intéressant de noter que ceux qui ont fait leurs études supérieures exclusivement en ligne souhaitent travailler sur site. Les CAE ont convenu que le fait de trouver un équilibre entre ces préférences conflictuelles est essentiel pour attirer et retenir le personnel.

Peu d'entreprises ont redéfini entièrement leurs processus de travail dans l'ère post-pandémie. Au lieu d'avoir de nouvelles attentes culturelles définies par les conseils d'administration, la culture est plus susceptible d'être définie par les cadres moyens par nécessité, dit Brian Tremblay, CAE chez 1stDibs. « La culture d'entreprise est définie par le « ton au milieu » où les gestionnaires prennent des décisions au profit de leurs gens, ce qui pourrait correspondre aux valeurs de l'entreprise ou non », dit-il. Les CAE peuvent contribuer en fournissant aux conseils d'administration des informations sur les différences des pratiques de travail à travers les unités opérationnelles de sorte que les conseils d'administration soient plus en harmonie avec les réalités culturelles.

Ressources

Gestion des talents: Recruter, former, motiver et retenir d'excellents joueurs d'équipe (IAI)

Cultiver une culture saine (Chartered Institute of Internal Auditors)

2023 Rapport sur l'éthique et la culture organisationnelle (Conseil d'audit)

[11] Pour plus de détails sur le Code DEI du secteur financier, veuillez vous rendre sur https://www.cfainstitute.org/en/about/press-releases/2023/dei-code-100-signatories-milestone

CAPITAL HUMAIN

La diversité n'est pas superficielle

Plusieurs recherches ont démontré une corrélation positive entre la diversité accrue et la croissance économique tant dans l'économie américaine en général que dans les entreprises individuelles.[12] De nombreuses entreprises ont souscrit à ces conclusions, ainsi que le gouvernement fédéral américain, qui met en œuvre de nouvelles exigences en matière de DEI pour les organismes fédéraux.[13]

Plusieurs CAE présents à la table ronde ont déclaré que leurs conseils d'administration s'attendent à ce que leurs entreprises aient largement recours aux indicateurs liés à la diversité et à l'inclusion. La CAE d'une banque de détail dit que son entreprise va au-delà du suivi d'attributs physiques et tient compte de la diversité en termes de pensée, d'approche et d'état d'esprit. Certaines entreprises utilisent le test de personnalité DiSC afin de mieux comprendre les styles de travail de leurs employés et d'optimiser l'efficacité des employés.[14]

Alors que le suivi de la diversité a des avantages, il faut être prudent pour éviter toute action judiciaire si la statistique démontre que certains groupes ont été victimes de discrimination.

Plusieurs CAE présents à la table ronde ont déclaré que leurs conseils d'administration s'attendent à ce que leurs entreprises aient largement recours aux indicateurs liés à la diversité et à l'inclusion

Chercher des signes de problèmes non traditionnels

La vérification des politiques, des procédures et des résultats des sondages auprès les employés sont des tâches d'audit interne évidentes, mais celles-ci peuvent manquer les signes de problèmes moins évidents. L'audit interne peut utiliser des observations judicieuses pour identifier les signes moins tangibles – moral bas, commentaires négatifs sur les réseaux sociaux, salles de repos désordonnées – et déterminer si ce sont des signes de problèmes culturels plus profonds.

Collaborer pour éliminer le recrutement cloisonné

Un CAE du secteur d'enseignement a fait écho à un sentiment croissant lorsqu'il a dit qu'il ne regardait plus l'audit interne comme un département cloisonné au sein de l'entreprise. Au lieu de cela, il a remanié la structure des ressources humaines de son département afin d'arrêter de prétendre que l'audit interne devait être une carrière à vie et nous a assuré qu'il a collaboré avec d'autres départements pour contribuer à l'amélioration de la rétention de l'ensemble du personnel, parce que tous les secteurs de l'entreprise sont soumis aux mêmes défis.

[12] Pour plus de détails sur la corrélation positive entre la diversité et le rendement, veuillez vous rendre sur https://hbr.org/2018/07/the-other-diversity-dividend

[13] Pour plus de détails sur la déclaration sur la DEI, veuillez vous rendre sur https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/25/executive-order-on-diversity-equity-inclusion-and-accessibility-in-the-federal-workforce/

Table des matières

Sommaire

CAPITAL HUMAIN

L'augmentation des rotations de l'intérieur de l'entreprise, l'utilisation accrue des services d'auditeurs invités pour des tâches spécifiques et la discussion ouverte des choix professionnels à long terme de nouveaux candidats ont contribué à réduire la pression de la fonction d'audit interne. « Je consacre la plupart de mon temps à aider les gens demeurer au sein de l'entreprise et bénéficier d'un environnement d'apprentissage, ce qui semble fonctionner », dit-il.

De la même façon, le CAE d'une entreprise d'analyse mondiale dit que son personnel fait souvent des mouvements latéraux à l'intérieur de l'entreprise après avoir eu un contact étroit avec de nombreuses unités opérationnelles. Malgré les efforts supplémentaires requis pour pourvoir les postes d'audit interne, il croit que les mouvements améliorent finalement la maturité aux risques de l'entreprise.

Profiter des points forts pour le recrutement de professionnels en audit interne

Alors que les CAE disent qu'ils s'efforcent d'aider les entreprises à créer une culture appropriée pour attirer, former et retenir des effectifs au sein de leurs entreprises,

« Je consacre la plupart de mon temps à aider les gens demeurer au sein de l'entreprise et bénéficier d'un environnement d'apprentissage ... »

beaucoup d'entre eux sont entravés par les pénuries d'effectifs et de compétences dans leurs propres fonctions d'audit – particulièrement dans les petites entreprises et le secteur public où les pressions budgétaires peuvent être intenses.

Bien que les entreprises du secteur public aient souvent du mal à offrir une rémunération compétitive, elles peuvent souligner l'esprit du service public afin d'améliorer le recrutement et la rétention d'effectifs, dit Pamela Stroebel Powers, la Directrice d'orientation professionnelle de l'IAI pour le secteur public. « Les entreprises doivent établir à l'avance des attentes en matière de rendement et s'assurer que les gens comprennent la façon dont leur travail se rapporte à l'objet de l'entreprise, parce que chaque poste au sein de l'entreprise devrait se rapporter à cette mission. »

CAPITAL HUMAIN

Comment l'audit interne peut aider l'entreprise

1. Évaluez la mesure dans laquelle la direction a identifié les risques émergents potentiels du travail hybride et a élaboré des stratégies et des politiques efficaces pour atténuer ces risques.
2. Évaluez les variétés des pratiques culturelles d'entreprise à l'échelle de l'entreprise et communiquez-les au conseil d'administration afin de contribuer à l'établissement du processus de prise de décisions et de politiques.
3. Évaluez l'utilisation des indicateurs de diversité formels et leur efficacité dans le suivi des politiques en matière de diversité et d'inclusion, notamment si elles englobent la diversité en termes de pensée et esprit.
4. Élaborez des stratégies pour utiliser les interactions personnelles avec les clients de l'audit afin d'identifier des signes intangibles que des problèmes culturels pourraient se produire et retenez ces observations pour le suivi et les mesures correctives.
5. Évaluez si la structure des ressources humaines de l'entreprise vise à attirer et retenir des talents au sein de l'entreprise – au lieu des cloisons individuels – et si les parcours professionnels sont bien structurés et clairement communiqués.
6. Évaluez si le but plus large de l'entreprise est bien défini et communiqué à travers l'entreprise, notamment dans les stratégies des ressources humaines visant à attirer et retenir des effectifs.

ÉVOLUTION DU MARCHÉ

Ajouter de la valeur par une participation stratégique

Les marchés changent de façon imprévisible, amenant les entreprises à investir dans des stratégies numériques qui répondent mieux aux tendances en évolution rapide. Les CAE réunissent les expertises de leurs entreprises et agissent comme conseillers sur les nouvelles initiatives pour contribuer à ces transformations.

L'économie en Amérique du Nord a entraîné l'évolution du marché, la concurrence et l'évolution du comportement des consommateurs pendant l'année écoulée. Au début de l'année 2022, la Federal Reserve (réserve fédérale) des États-Unis a détourné son attention de la pandémie à la maîtrise de l'inflation, marquant ainsi la fin d'une époque d'argent historiquement à bon marché. Les faillites commerciales ont augmenté parce que l'aide fourni durant la pandémie est disparu et les clients ont réduit leurs dépenses en raison des hausses de prix.[15] L'inflation et la hausse du dollar ont rendu les produits fabriqués en Amérique du Nord plus chers, en réduisant les marges nationales et en amenant l'importation – notamment de la Chine – aux niveaux pré-pandémie.[16] Dans le secteur des services financiers, certaines banques se sont effondrées partiellement parce qu'elles n'ont pas réussi à gérer le risque de taux d'intérêt.[17]

En même temps, les entreprises s'adaptent aux tendances à long terme en consumérisme numérique. Les jeunes ont transformé la façon dont les consommateurs interagissent avec les entreprises – de l'activité d'achat et d'utilisation de services à l'activisme et à la critique publique. Sur un marché moins fidèle et plus connecté socialement, les réputations risquent d'être ternies et de déclencher des rues sur les banques en quelques heures.

Résultats du sondage – Évolution du marché:

4ÈME – NIVEAU DE RISQUE

41% l'ont classée dans les premiers 5 *pour le niveau de risque*

13ÈME – EFFORT D'AUDIT

14% l'ont classée dans les premiers 5 *pour l'effort d'audit*

[15] Pour plus de détails sur les indicateurs de faillite aux États-Unis, veuillez vous rendre sur https://tradingeconomics.com/united-states/bankruptcies
[16] Pour plus de détails sur le commerce mondial, veuillez vous rendre sur https://www.globaltrademag.com/increase-in-u-s-container-import-volumes-makes-2023-look-more-like-2019/
[17] Pour plus de détails sur les faillites bancaires, veuillez vous rendre sur https://www.nytimes.com/article/svb-silicon-valley-bank-explainer.html

Table des matières

Sommaire

ÉVOLUTION DU MARCHÉ

L'intervention précoce permet de prévenir les problèmes futurs

Les investissements promptes dans la technologie pour la fourniture de produits et services sont souvent indispensables pour rester en phase avec le marché, disent les CAE présents à la table ronde. Mais cela augmente l'exposition à d'autres menaces, notamment la cybersécurité pour les systèmes neufs et non encore testés et le risque lié à la chaîne d'approvisionnement où les services migrent vers le nuage ou changent leur structure opérationnelle.

C'est pourquoi il est essentiel que les CAE soient impliqués comme conseillers dans la phase de mise en œuvre, dit Ada Leung, Vice-presidente et CAE chez Fidelity au Canada. « Il ne suffit plus de revenir trois années après le lancement d'un projet et de s'assurer que les contrôles étaient satisfaisants. Aujourd'hui, nous travaillons en collaboration et en partenariat avec nos associés pour garantir les contrôles de conception avant la mise en œuvre. C'est une approche beaucoup plus sûre, moins chère et plus efficace. »

> « L'évolution du marché représente un événement de risque dynamique en soi, donc les CAE doivent être rester vigilants en permanence pour réévaluer ce qu'ils vérifient et la façon dont ils le font. »

Mais l'élaboration d'un plan d'audit pour une entreprise en pleine transformation numérique est difficile. « Les CAE doivent être assimilés aux stratégies organisationnelles, ce qui signifie ne pas mener d'évaluations des risques statiques et ne pas avoir un plan d'audit événementiel inflexible », dit Harold Silverman, Directeur principal des CAE et de l'engagement de la gouvernance d'entreprise de l'IAI. « Les technologies émergentes et l'évolution du marché représentent des événements de risque dynamiques à eux seuls, donc les CAE doivent être rester vigilants en permanence pour réévaluer ce qu'ils vérifient et la façon dont ils le font. » Au lieu de se concentrer uniquement sur des engagements individuels, Silverman dit que les CAE doivent mettre à jour leurs tâches d'audit régulièrement de sorte, que qu'ils intègrent ces nouveaux éléments au calendrier prévisionnel des travaux du département d'audit.

C'est logique, d'abord parce que les risques liés à l'évolution du marché sont souvent inhérents à d'autres types de menaces, par exemple, le risque financier et de liquidités. Deuxièmement, l'intégration des risques du marché dans le calendrier prévisionnel des travaux peut aider un CAE à prévenir ce risque sans devoir l'aborder avec un comité d'audit réticent – même si l'éducation aux risques en croissance représente une importante fonction du CAE. Finalement, il empêche le département d'audit interne de négliger les menaces émergentes en raison d'un plan d'audit périmé ou de méthodologies lentes qui ne correspondent pas à la catégorie de risque, dit-il.

ÉVOLUTION DU MARCHÉ

Calculer les coûts des risques du marché

Les entreprises doivent faire faire plus que simplement identifier les risques du marché; elles doivent calculer des informations précises et spécifiques sur les impacts financiers, dit le CAE d'une entreprise de soins de santé à but non lucratif. « Mon objectif est de savoir « Quel est notre risque non négligeable en termes de dollars? » de sorte que notre équipe de haute direction puisse décider des initiatives stratégiques à poursuivre ou non. »

Ayaka Mitsunari, Directeur d'audit interne – Architecte de risque pour la livraison chez Uber, dit que son équipe examine les processus de gouvernance, la stratégie et les structures opérationnelles afin de déterminer si l'entreprise est capable de répondre aux défis du marché de manière efficace. Par exemple, l'audit interne demande « Comment la direction mesure-t-elle l'adhésivité du produit? Ont-ils les bons processus pour pouvoir s'adapter de manière rapide et innovante? » dit-elle.

Faire appel aux experts si nécessaire

Compte tenu de la nature interconnectée du risque et de ses stratégies d'atténuation, la collaboration à travers l'entreprise en profitant des sources de connaissances est la clé du succès. « Compte tenu de l'évolution accélérée des marchés et des tendances des clients, l'avenir pour les professionnels de l'audit interne et de la gestion des risques est de pouvoir collaborer avec les cadres supérieurs pour atténuer dans six mois un risque que vous n'avez pas encore identifié. Voulez allez changer et être flexible », dit un universitaire de premier plan présent à la table ronde.

« Nous n'avons pas toutes les réponses dans ces domaines émergents, donc nous devons être humbles, apprendre et connaître les domaines de risques où nous devons faire appel aux experts s'il existe des faiblesses dans l'entreprise », Nancy Russell, CAE chez Canada Life. « Cela pourrait se heurter aux egos de la direction, mais il est important de les encourager à être transparents avec le conseil d'administration là ou il n'y a pas de solutions et à être ouverts à demander de l'aide si nécessaire. »

Afin de construire des connaissances commerciales, les CAE présents à la table ronde dit qu'ils s'efforcent d'embaucher une cohorte diversifiée d'effectifs, surtout ceux avec un sens aigu des affaire et expérience – bien que les pénuries actuelles en matière de compétences et talents rendent cette tâche difficile. Afin d'élargir l'étendue et la profondeur des compétences en audit interne, ils disent également qu'ils se sont concentrés sur la stimulation de la certification et de la formation, ainsi que sur la rotation des employés à travers le département et l'utilisation des services d'auditeurs invités pour les problèmes techniques.

Table des matières

Sommaire

ÉVOLUTION DU MARCHÉ

Comment l'audit interne peut aider l'entreprise

1. Évaluez la gestion des risques de l'entreprise pour vous assurer qu'ils ont en place des processus d'analyse prospective adéquats pour suivre les tendances émergentes du marché et les utiliser pour la prise de décisions stratégiques.
2. Formulez des commentaires sur les projets technologiques axés sur le marché au stade de l'exécution pour vous assurer que les risques sont évalués et atténués de manière appropriée.
3. Évaluez l'efficacité avec laquelle les risques liés à l'évolution du marché, à la concurrence et au comportement des consommateurs sont quantifiés en termes monétaires et utilisés dans des processus de prise de décisions.
4. Évaluez dans quelle mesure les processus de gouvernance globale de l'entreprise répondent à l'évolution du marché et peuvent se transformer afin de profiter de nouvelles opportunités.
5. Évaluez les stratégies en matière de ressources humaines de l'organisation pour vous assurer que les compétences et les expertises clés ayant trait aux risques et opportunités futurs sont identifiés – notamment dans le département d'audit interne – et recrutés en temps utile.

Table des matières

Sommaire

CONTINUITÉ D'ACTIVITÉ

Renforcer la résilience en complexité

Si les conseils d'administration avaient tendance à sous-privilégier les plans de continuité d'activité avant la pandémie, ce n'est plus le cas. Les cyberattaques de grande envergure, les phénomènes météorologiques extrêmes et les tensions géopolitiques croissantes – surtout entre les États-Unis et la Chine – continuent à garder le point à l'ordre du jour.

En fait, la continuité d'activité, la résilience opérationnelle, la gestion des crises et la reprise sur sinistre sont rarement considérées comme des risques à eux seuls, mais comme une réponse à un large éventail d'interruptions d'activité potentielles. « Pour les risques systémiques auxquels nous sommes confrontés et les menaces telles que la perturbation des chaînes d'approvisionnement et la résilience des fournisseurs, nous considérons que la réponse à tous ces différents aspects est d'avoir un plan de continuité d'activité », dit le CAE d'un fabricant américain.

La planification basée sur des événements réduite

L'expérience de la pandémie et les changements macroéconomiques rapides qui ont accéléré l'inflation et les taux d'intérêt non seulement ont mis en évidence l'impérieuse nécessité que les conseils d'administration préparent les entreprises pour l'avenir de manière plus efficace, mais ont changé également la façon dont les entreprises pensent à la résilience opérationnelle.

Résultats du sondage – Continuité d'activité

5ÈME – NIVEAU DE RISQUE

36% l'ont classée dans les premiers 5 *pour le niveau de risque*

3ÈME – EFFORT D'AUDIT

53% l'ont classée dans les premiers 5 *pour l'effort d'audit*

CONTINUITÉ D'ACTIVITÉ

En particulier, les CAE présent à la table ronde ont convenu que la pandémie a bouleversé surtout les plans de continuité d'activité existants en raison de l'échelle et de la complexité de l'événement. Les organismes du secteur public, par exemple, ont dû distribuer des aides gouvernementales immédiatement sans avoir des contrôles de la fraude en place. En outre, les fournisseurs, les partenaires et les clients ont été affectés également, donc, le plus souvent, les plans de continuité d'activité n'ont pas réussi à expliquer les perturbations aux entreprises vers lesquelles ils se tourneraient normalement pour obtenir du soutien.

« Mon entreprise avait fait beaucoup en matière de préparation aux catastrophes et de planification pour les catastrophes locales, mais cela a frappé tout le monde subitement, donc les entreprises n'étaient pas préparées pour les urgences interfonctionnelles, pangouvernementales d'une telle envergure », dit Pamela Stroebel Powers, la Directrice d'orientation professionnelle de l'IAI pour le secteur public. Les entreprises ont appris que les risques subits, imprévisibles, en cascade représentent la principale caractéristique des risques systémiques. Cela signifie que les catastrophes qui sont systémiques – plutôt que déclenchées par un seul événement, par exemple une tempête – changent fondamentalement la façon dont ce risque peut être géré et atténué pendant une crise.

Les entreprises doivent planifier tant pour les crises basées sur des événements et non traditionnelles à large portée. Shannon Urban, Vice-présidente et CAE chez Hasbro, dit que son entreprise a élargi le programme pour la gestion des risques d'entreprise de sorte à inclure les deux types de risque et l'audit interne garantit qu'ils y sont inclus, suivis et que des plans de reprise sur sinistre sont en place. De plus, les plans de reprise sur sinistre font l'objet d'exercices de simulation sur ordinateur réguliers, où l'audit interne peut soulever des inquiétudes de sorte que toute faiblesse soit identifiée et gérée d'une manière proactive.

Les évaluations de risques détaillées exigent une collaboration plus profonde

Étant donné que l'incertitude macroéconomique et géopolitique, l'évolution du marché, les phénomènes de changement climatique et le risque de cybersécurité ont des caractéristiques similaires en termes de rapidité, évolutivité et complexité, les entreprises redéfinissent les paramètres de leurs plans de réaction aux catastrophes et se concentrent davantage sur la résilience organisationnelle. Quelques CAE présents à la table ronde disent qu'ils se sentent actuellement en crise permanente, mais avec des ressources limitées. Dans certains secteurs, les organismes de réglementation insistent que les entreprises adoptent une position à plus long terme sur leur viabilité.

> Les entreprises doivent planifier tant pour les crises basées sur des événements et non traditionnelles à large portée.

CONTINUITÉ D'ACTIVITÉ

« Bien que le rythme des changements semble rapide maintenant, c'est probablement le plus lentement que nous fonctionnerons, car des développements tels que l'IA vont accélérer plus rapidement », dit Nancy Russell, CAE chez Canada Life. « Nous devons découvrir les éléments avec lesquels nous et les organismes de réglementation sommes à l'aise et ce que la résilience opérationnelle signifie concrètement – et en raison de la dynamique des changements au sein de l'entreprise, nous devons devenir à l'aise également avec le fait de ne pas nous sentir à l'aise. »

Dans le cadre de ces efforts, les entreprises doivent réajuster les évaluations des risques afin de relier de façon créative les menaces apparemment sans rapport ou inattendues qui, ensemble, pourraient interrompre leurs activités. Par exemple, le CAE d'une société technologique américaine dit que 80% de la capacité de fabrication de puces de son entreprise était basée à Taiwan, qui est potentiellement menacée par la Chine. Il avait utilisé la planification de scénarios sur ordinateur pour créer une image exacte de la façon dont la société pourrait agir afin de répondre aux demandes des clients à la lumière d'une guerre potentielle, des sanctions ou de perturbation des chaînes d'approvisionnement. « Le fait d'avoir des plans de continuité et des pratiques de résilience en place soit pour réagir soit pour se préparer à l'avance a vraiment contribué à cibler les efforts des conseils d'administration en matière de résilience sur le plan stratégique », dit-il.

L'ajout de détails riches dans ces scénarios est essentiel, parce que les atténuations suivant à la gestion des menaces peuvent elles-mêmes créer des risques de deuxième et troisième ordre qui doivent être atténués – mais cela implique une collaboration plus approfondie avec la direction sur ce qui peut tourner mal. « Lorsqu'il s'agit de crises, nous avons élargi nos réunions pour l'évaluation des risques, parce que cela aide les dirigeants à se préparer vraiment pour les questions à plus long terme », dit le CAE d'un établissement d'enseignement supérieur. Les entreprises vont s'effondrer en cas de catastrophe si elles ne travaillent pas ensemble pour créer ces plans détaillés, basés sur des données.

« Il est plus important que jamais de rencontrer les gestionnaires en personne et de prendre le pouls de ce qui les empêche de dormir, ainsi que de partager le suivi de l'audit interne », dit Hasbro's Urban. « Neuf fois sur dix, vous n'avez pas besoin d'un audit formel pour stimuler le changement – il suffit de convaincre les bonnes personnes que le problème est vraiment quelque chose à quoi elles devraient penser. »

Les CAE présents à la table ronde disent qu'ils ont soutenu également la robustesse des évaluations de risques, des structures de gouvernance et de la pertinence des plans de continuité d'activité, et se sont assurés que des ressources sont en place pour mettre en œuvre le plan en cas de catastrophe. Beaucoup d'entre eux disent qu'ils ont mis en œuvre une forme d'assurance combinée pour la planification de la continuité de leur activité, et certains d'entre eux disent qu'ils ont collaboré avec des experts externes et fournisseurs pour s'assurer qu'ils avaient le moins de lacunes possibles dans l'éventail d'événements couverts et dans leurs plans.

Ressources

Gestion de la continuité d'activité (L'IAI)

Gestion des risques géopolitiques (Chartered Institute of Internal Auditors)

Verification de la gestion des risques des tiers (L'IAI)

Table des matières

Sommaire

CONTINUITÉ D'ACTIVITÉ

La planification à l'avance pour combler les postes est essentielle

La complexité de ces menaces à grande échelle exige une planification de la continuité opérationnelle basée sur de hauts niveaux d'expertise dont les entreprises ne disposent pas souvent dans la crise actuelle de ressources humaines – le capital humain, la diversité et la gestion et la rétention de talents sont classés dans le sondage comme la deuxième plus importante menace. Les compétences clés et les talents sont insuffisants. Les modèles économiques allégés et l'automatisation ont supprimé certaines ressources requises pour un travail tellement détaillé, disent les CAE présents à la table ronde.

En outre, la planification de la relève pour les postes de gestion clés constitue un risque émergent. Il est courant que les postes de direction vacants difficiles à pourvoir soient ouverts pendant plus d'un an, surtout dans les domaines comme la technologie de l'information et dans de nombreuses autres spécialisations dans les petites entreprises et les organismes du secteur public. « Nous tentons de faire de plus en plus avec moins, donc nous ne pouvons pas offrir des salaires compétitifs », dit le CAE d'une université.

« Il n'existe aucun plan de relève en place pour les rôles clés et cela se répercute sérieusement sur la continuité d'activité. » Si des rôles clés sont attribués à ces postes dans les plans, cela ne fonctionnera pas si une urgence survient: la personne qui occupe un tel poste doit reconnaître le sinistre et doit avoir exercé les mesures d'intervention.

La préparation pour les réglementations sur les risques émergents qui pourraient perturber l'activité de l'entreprise ou de ses chaînes d'approvisionnement, comme les futures sanctions américaines - chinoises, exige que les entreprises embauchent des experts à l'avance. Le CAE de l'entreprise de production connectée de Taiwan dit que son entreprise s'orientait plus vers le développement logiciel et avait besoin non seulement de faire des embauches pour un changement de direction stratégique, mais aussi de s'assurer que l'entreprise disposait de l'expertise réglementaire nécessaire pour l'intégrer dans ses exercices de planification pour la continuité d'activité.

Compte tenu de l'incertitude mondiale croissante, il n'est peut-être pas surprenant que, dans trois années, les répondants au sondage s'attendaient à ce que la continuité d'activité ne soit classée que 3 points de pourcentage moins qu'aujourd'hui – en baisse de 38% à 35% de personnes qui la considèrent l'un des 5 premiers risques. Pourtant, les CAE s'attendaient à ce que leurs départements d'audit interne consacraient moins de temps à traiter la question: le nombre de

ceux qui estimaient qu'il serait un point prioritaire des 5 premiers risques a baissé de 54% à 46% dans trois années. La plupart des CAE présents à la table ronde disent qu'ils s'efforçaient à intégrer le sujet de la continuité d'activité dans tous les audits internes futurs – bien que les deux plus importants secteurs de risques émergents – la perturbation numérique et le – constituent potentiellement des problèmes de continuité d'activité qui pourraient exiger plus d'attention que prévu.

Table des matières

Sommaire

CONTINUITÉ D'ACTIVITÉ

Comment l'audit interne peut aider l'entreprise

1. Évaluez la mesure dans laquelle le cadre de gestion des risques d'entreprise comprend des risques de perturbation basés sur des événements et à grande échelle.
2. Comparez les exigences réglementaires avec l'appétence au risque de l'entreprise afin de déterminer une stratégie appropriée pour la planification de la continuité d'activité.
3. Aidez à identifier les risques de deuxième et troisième ordre qui pourraient survenir dans des scénarios de risque complexes ou en raison de l'impact négatif des mesures d'atténuation de premier ordre dans le plan de continuité d'activité.
4. Examinez les processus de la continuité d'activité pour vous assurer qu'une large diversité de voix et d'experts contribuent au brainstorming et à l'élaboration du plan afin d'adopter une perspective à plus long terme.
5. Venez au soutien de la direction en offrant une opinion indépendante et critique lors des exercices sur ordinateur pour évaluer leur exhaustivité et pour souligner les aspects dans lesquels les plans d'atténuation des risques ont besoin de ressources ou de tests supplémentaires.
6. Donnez l'assurance que les ressources et le personnel identifiés dans les plans de reprise sur sinistre et de gestion des crises sont en place et que les processus et les contrôles qui appuient ces plans existent et fonctionnent pendant les exercices en temps réel.
7. Évaluez les besoins en capital humain de l'entreprise pour une planification efficace de la continuité d'activité, notamment l'existence du personnel clé et de l'expertise dans des domaines de risques émergents ainsi que dans le département d'audit interne.

RISQUES INTERCONNECTÉS

Incertitude géopolitique, chaîne logistique et changements réglementaires

Les efforts de gérer les vastes répercussions des risques mondiaux émergents sont entravés par l'intensification des exigences réglementaires. Les CAE cherchent une meilleure harmonisation à la gestion des risques dans des domaines complexes, tels que la perturbation des chaînes d'approvisionnement.

Participer à des discussions sur la planification stratégique pour l'incertitude géopolitique

Les CAE présents à la table ronde disent que de nombreuses entreprises américaines de Fortune 100 ont le risque de guerre sur leur radar. Influencées par l'invasion inattendue de l'Ukraine par la Russie en 2022 et les tensions croissantes avec la Chine, les entreprises ont renforcé leurs défenses en matière de cybersécurité et ont réexaminé les évaluations des risques et les scénarios à travers un large éventail de menaces interconnectées, disent-ils.

Cependant, tout comme beaucoup d'autres menaces interconnectées dans ce rapport, ce serait une erreur de classer le risque macroéconomique et géopolitique comme une simple catégorie de risque individuelle.

Si le Brésil, la Russie, l'Inde, la China et l'Afrique du Sud, par exemple, ont lancé une monnaie mondiale alternative largement discutée qui pourrait, tout comme d'autres décisions géopolitiques, être un facteur clé pour un ensemble de risques connexes qui pourraient frapper les entreprises nord-américaines de manière imprévisible, subite et simultanée à travers toutes leurs structures.[18]

Donc, bien que cette catégorie se soit classée en bas de la liste en termes de temps et d'efforts consacrés à l'audit, ces efforts sont très probablement distribués dans des activités qui pourraient ne pas se retrouver dans le plan d'audit, par exemple, les tests de stress l'analyse de scénarios et les conseils stratégiques.

Le CAE d'un cabinet-conseil mondial nord-américain de premier plan dit: « Il existe une différence entre ce qui peut être vérifié dans votre plan d'audit par rapport à votre rôle au sein de l'entreprise, surtout lorsque vous participez à des réunions de planification stratégique. » Il dit que les CAE doivent agir comme des catalyseurs stratégiques pour le conseils d'administration de sorte qu'ils prennent des décisions éclairées et promptes dans ces scénarios de risque à évolution rapide, mais à long terme.

« Il existe une différence entre ce qui peut être vérifié dans votre plan d'audit par rapport à votre rôle au sein de l'entreprise, surtout lorsque vous participez à des réunions de planification stratégique. »

[15] Pour plus de détails sur la monnaie BRICS, veuillez vous rendre sur https://foreignpolicy.com/2023/04/24/brics-currency-end-dollar-dominance-united-states-russia-china/

RISQUES INTERCONNECTÉS

Diversifier la chaîne d'approvisionnement avant que la crise ne se déclenche

Alors que la pandémie a exposé les faiblesses des réseaux de chaînes d'approvisionnement mondiaux, par exemple par la fermeture des ports et l'interruption des flux commerciaux, l'Amérique du Nord dépend toujours de la Chine pour une grande partie de sa production. En 2023, la Chine a réalisé 28,4% de la production manufacturière mondiale par rapport à 16,6% aux États-Unis – en dollars, 4 trillions de dollars et respectivement 1,8 trillions de dollars.[19] Les événements récents ont mis en évidence le fait qu'un nombre trop grand d'entreprises sont affectées par d'importants risques en ce qui concerne les fournisseurs clés. C'est peut-être l'un des motifs pour lesquels le discours politique a changé de la séparation de la Chine à la diversification et la résilience des chaînes d'approvisionnement.[20] Le défi n'est pas seulement de trouver un fabricant dans un autre lieu, mais il est plus important de transformer l'entière infrastructure opérationnelle afin d'éviter les problèmes logistiques et de qualité potentiels.[21]

> « Il ne suffit pas d'acquérir des connaissances pour la fabrication de produits de haute qualité d'un pays qui fait cela depuis 50 années et les transposer dans un pays qui fait cela depuis 10 années. »

Par exemple, lorsque la société global mondiale de jeux et jouets a commencé sa diversification en dehors de la Chine il y a quelques années, ils ont dû faire d'importants investissements à travers leur entière structure opérationnelle ainsi qu'auprès des partenaires tiers. « Il ne suffit pas d'acquérir des connaissances pour la fabrication de produits de haute qualité d'un pays qui fait cela depuis 50 années et les transposer dans un pays qui fait cela depuis 10 années », dit Shannon Urban, Vice-presidente et CAE chez Hasbro. Les partenariats visant à former le personnel des fournisseurs et la duplication d'outils à plusieurs endroits ont facilité le processus et ont introduit une résilience supplémentaire dans l'entreprise.

L'initiative lancée chez Hasbro faisait partie d'un programme de transformation plus

ample, mené par la direction, à travers l'entière infrastructure de la chaîne d'approvisionnement, dans le but de renforcer la résilience à toutes les échelles de l'entreprise – un projet stratégique essentiel. Étant donné que l'automatisation était un élément clé de l'initiative, l'audit interne s'est impliqué dans le projet pour fournir des conseils sur la conception de contrôles efficaces pour ces systèmes et a repensé les processus et les contrôles dès le début. Ce type de travail exige un ensemble de compétences différentes de celles de l'audit interne traditionnel, donc Hasbro a investi dans l'évaluation des compétences et la formation en cours d'emploi pour l'équipe d'audit.

[19] Pour plus de détails sur l'analyse de la production de U·S· Statistical Division, veuillez vous rendre sur https://worldpopulationreview.com/country-rankings/manufacturing-by-country
[20] Pour plus de détails sur la déclaration sur la diversification, veuillez vous rendre sur https://www.reuters.com/world/cias-burns-us-needs-de-risk-diversify-away-china-2023-07-01/
[21] Pour plus de détails sur les défis de transplanter la production, veuillez vous rendre sur https://asiatimes.com/2023/06/why-so-much-manufacturing-still-gets-done-in-china/

RISQUES INTERCONNECTÉS

Essayer d'obtenir une harmonisation et de l'aide pour les risques contradictoires

Les CAE présents à la table ronde ont convenu que les réglementations compliquaient la restructuration des chaînes d'approvisionnement. L'augmentation du risque prévu pour les changements réglementaires est probablement alimentée par la prolifération de lois sur la protection des données de type européen à travers l'Amérique du Nord. Contrairement à l'Europe où le Règlement général sur la protection des données de 2018 est mis en œuvre avec peu de modifications par les pays de la région, les législateurs nord-américains ont pris ces concepts et ont promulgué des règles très différentes d'État à État tout en créant un patchwork d'exigences souvent contradictoires en matière de conformité.[22]

« Nous sommes arrivés à une situation où le fait de fournir une assurance absolue sur les lois en matière de confidentialité des données est tellement exorbitante qu'il est presque impossible », dit Brian Tremblay, CAE chez 1stDibs. Il a comparé la situation actuelle concernant la confidentialité des données aux débuts de la conformité SOX, où le secteur était tellement réglementé qu'il absorbait trop d'effort de l'audit interne.

Les CAE présents à la table ronde ont convenu que le temps de l'audit interne est trop divisé pour gérer efficacement les risques émergents et les exigences de conformité croissantes en même temps. « Au moment ou nous répondons à ces changements de comportement des clients et investissons dans la technologie, le rythme des changements réglementaires au niveau fédéral et d'État est devenu incontrôlable », dit une CAE du secteur des soins de santé. Selon elle, cette pression avait rendu son entreprise plus réactive, en indiquant une raison pour laquelle le temps de l'audit interne est souvent réaffecté à la conformité réglementaire.

L'harmonisation de l'audit interne et de la gestion des risques est essentielle, dit Tremblay. Comme de nombreux CAE des entreprises cotées en bourse, il est responsable de la gestion des risques. Dans le cadre de son rôle, il contribue à définir l'appétence au risque et les politiques de confidentialité et à documenter la façon dont ces décisions pourraient fournir une meilleure clarté sur la position de l'entreprise. La collaboration avec le département informatique pour utiliser des solutions à l'échelle de l'entreprise visant à intégrer des contrôles de confidentialité doit constituer une stratégie clé si les auditeurs internes ne sont pas surchargés par le travail lié à la conformité, ajouta-t-il.

[22] Pour plus de détails sur les lois en matière de confidentialité à implémenter en 2023, veuillez vous rendre sur https://secureprivacy.ai/blog/2023-us-consumer-privacy-laws

RISQUES INTERCONNECTÉS

Comment l'audit interne peut aider l'entreprise

1. Soutenez le conseil d'administration dans la planification stratégique afin de contribuer à faciliter la prise de décisions éclairées en matière de risques géopolitiques et économiques émergents et à évolution rapide.
2. Évaluez les processus de l'entreprise afin d'identifier, d'évaluer et d'élaborer des stratégies d'atténuation pour les risques géopolitiques complexes et encouragez-les à prêter attention aux interconnexions entre les catégories de risque.
3. Évaluez la stratégie de l'entreprise en matière de chaînes d'approvisionnement, notamment si elle a évalué de manière adéquate les risques liés à l'infrastructure locale critique lors de l'implantation dans d'autres régions.
4. Évaluez la relation de l'entreprise avec les fournisseurs essentiels et évaluez la nécessité d'une approche plus collaborative en termes de formation et de renforcement des capacités.
5. Évaluez la communication entre les départements de gestion des risques et d'audit interne afin de mieux harmoniser le suivi des risques émergents.
6. Évaluez la maturité des systèmes de contrôle automatisés de l'entreprise afin de contribuer à réduire le fardeau de la conformité réglementaire.

ATTENTES POUR L'AVENIR

La pression augmente en raison de la perturbation numérique et du changement climatique

Deux secteurs se sont distingués considérablement en ce qui concerne les risques attendus en termes de risques et d'efforts d'audit – la perturbation numérique et le changement climatique. Les CAE aident leurs entreprises à mieux les comprendre et gérer et les aident également à maintenir une perspective stratégique.

Les progrès rapides de l'intelligence artificielle en 2023 ont été mis en évidence par l'énorme couverture médiatique de l'algorithme ChatGPT de Open AI, un programme qui crée des documents écrits sur demande.[23] Les participants à la table ronde disent qu'ils ont fait testé soigneusement le programme. « Nous n'avons utilisé ChatGPT que pour poser des questions, mettre en contexte et rédiger des articles », dit le CAE d'une chaîne de détail. « Nous l'avons utilisé même pour certaines des discours du conseil d'administration et pour la rédaction, mais avec beaucoup de prudence. » Personne ne s'y est fié entièrement pour la création de documents, mais le CAE d'une entreprise de soins de santé à but non lucratif dit que cela a accéléré sa recherche et la préparation de rapports.

L'attraction est évidente – ces technologies peuvent améliorer la productivité, la compétitivité et même améliorer les marges à une époque de coûts de production élevés et de crise liée au coût de la vie. Mais les CAE présents à la table ronde ont convenu que les utilisateurs ne comprennent pas toujours les risques potentiels, tels que la violation des lois en matière de conformité des données ou l'introduction d'éléments de partialité dans les processus de prise de décisions. Étant donné qu'il est facile de télécharger et d'utiliser ces technologies, il est difficile de se tenir au courant de ces risques.

Résultats du sondage – Attentes pour l'avenir

PERTURBATION NUMÉRIQUE	Le niveau de risque a augmenté du 9ème au 2ème
CHANGEMENT CLIMATIQUE	Le niveau de risque a augmenté du 15ème au 9ème

[23] Pour plus de détails sur ChatGPT, veuillez vous rendre sur https://www.sciencefocus.com/future-technology/gpt-3/

ATTENTES POUR L'AVENIR

Risque informatique émergent pour l'audit au rythme de la technologie

« Le défi clé pour les auditeurs interne est de s'assurer qu'ils font des vérifications au rythme de la technologie, parce que les technologies perturbantes n'ont généralement pas en place de politiques, procédures, méthodologies, évaluations des risques et atténuations pour une TI plus mieux établie », dit Harold Silverman, Directeur principal des CAE et de l'engagement de la gouvernance d'entreprise de l'IAI. Ceci exige non seulement d'y être présent avec les connaissances adéquates lorsque ces projets commencent au sein de l'entreprise, mais aussi embaucher des personnes avec des compétences appropriées dans le département d'audit.

> « Au lieu de discuter simplement du risque d'un point de vue négatif, les CAE devraient être disposés à avoir une conversation sur les avantages potentiels pour un meilleur accent sur l'ESG. »

La clé est de garder le contrôle sur la gouvernance de données. Le groupe de discussion a convenu que la gouvernance de données peut être difficile à comprendre dans les entreprises à évolution rapide. Cela a conduit certaines entreprises à diviser leurs définitions de la gouvernance en plusieurs sections de gestion – la gouvernance de données IP, la gouvernance de données de confidentialité et ainsi de suite. L'examen transversal de ces sujets mineurs des différents audits peut aider, de même que l'intégration de contrôles pour la confidentialité des données dans les processus automatisés.

Le signalement des risques liés au changement climatique exige une perspective stratégique

Le fait d'avoir des données précises et des rapports hiérarchiques sera critique lorsque les entreprises commencent à s'attaquer aux risques climatiques. L'amélioration de la divulgation est en cours de préparation par la SEC, et les grands contribuables (entreprises avec une émission d'actions de 700 millions de dollars) doivent faire des déclarations sur les émissions de gaz à effet de serre et d'autres indicateurs de l'exercice financier terminé en 2023.[24] Les petites entreprises commencent à soumettre leurs déclarations en 2024. Mais les entreprises nord-américaines sont moins actives dans ce secteur que d'autres régions du monde. Avec tant de risques élevés stressants sur l'ordre du jours des entreprises, les CAE doivent faire preuve de prudence afin d'informer le conseil d'administration et de commencer des conversations qui les aideront à se préparer.

« Les CAE doivent avoir l'esprit ouvert à l'égard de l'évaluation des risques liés aux sujets ESG (environnemental, social et gouvernance) et discuter avec les cadres supérieurs et leurs conseils d'administration au sujet de ces risques, même d'une perspective stratégique », dit Richard Chambers, Conseiller principal en audit chez AuditBoard. « Au lieu de discuter simplement du risque d'un point de vue négatif, les CAE devraient être disposés à avoir une conversation sur les avantages potentiels pour un meilleur accent sur l'ESG. »

Ressources

Vérification des risques de confidentialité (L'IAI)

Analyser l'audit interne par rapport au risque de changement climatique (Chartered Institute of Internal Auditors)

[24] Pour plus de détails sur les réglementations climatiques de la SEC, veuillez vous rendre sur https://www.sec.gov/files/33-11042-fact-sheet.pdf

Table des matières

Sommaire

ATTENTES POUR L'AVENIR

Comment l'audit interne peut aider l'entreprise

1. Discutez avec la direction au sujet des technologies émergentes afin de donner des conseils en matière de risques et contrôles pour la mise en œuvre de nouveaux systèmes.
2. Évaluez la façon dont la direction structure et apprécie les données, notamment si la taxonomie des données est suffisamment détaillée pour identifier et atténuer les risques appropriés.
3. Donnez l'assurance que l'entreprise identifie des systèmes et processus informatiques fondamentaux qui peuvent être utilisés pour intégrer des contrôles de la confidentialité et des données afin de réduire le fardeau de la conformité à travers les trois axes.
4. Évaluez l'exhaustivité et l'exactitude des processus de données de l'entreprise qui ont trait aux questions d'ESG, avec une attention particulière aux nouvelles exigences réglementaires en matière de conformité pour les divulgations de nature climatique.
5. Discutez avec le conseil d'administration des questions relatives à ESG de manière proactive – et d'autres risques émergents – en mettant l'accent sur les avantages potentiels d'adopter une position stratégique proactive d'utilisateur précoce.

REMERCIEMENTS

L'équipe équipe chargée de la rédaction du rapport en Amérique du Nord

Directeurs de projet
Laura LeBlanc –
Directrice principale, Internal Audit Foundation
Deborah Poulalion –
Directrice de recherche & insights, L'IAI
Emely Katz – Directrice, Engagement des affiliés, L'IAI

Analyse de sondages et développement de contenus
Deborah Poulalion –
Directrice de recherche & insights, L'IAI

Résacteur de recherche
Arthur Piper –
Smith de Wint, le Royaume-Uni

Graphiste
Cathy Watanabe

Modérateur de la table ronde – Amérique du Nord
Harold Silverman –
Directeur principal, CAE et Engagement de la gouvernance d'entreprise, L'IAI

Traduction en français
L'Institut des auditeurs internes du Canada

Promoteur des rapports en Amérique du Nord
AuditBoard

Internal Audit Foundation 2023–24 Conseil d'administration

Président
Warren W. Stippich Jr., CIA, CRMA

Vice-président principal – Stratégie
Glenn Ho, CIA, CRMA

Vice-président – Finances et développement
Sarah Fedele, CIA, CRMA

Vice-président – Contenu
Yulia Gurman, CIA

Administrateurs
Hossam El Shaffei, CCSA, CRMA
Reyes Fuentes Ortea, CIA, CCSA, CRMA
Nora Kelani, CIA, CRMA
Shirley Livhuwani Machaba, CCSA, CRMA
Raoul Ménès, CIA, CCSA, CRMA
Hiroshi Naka, CIA
Anthony J. Pugliese, CIA
Bhaskar Subramanian

Équipe de liaison
Laura LeBlanc –
Directrice principale, Internal Audit Foundation

Internal Audit Foundation 2023–24 Commité des conseillers en recherche et éducation

Présidente
Yulia Gurman, CIA

Vice-présidente
Jane Traub, CIA, CCSA, CRMA

Membres
Tonya Arnold-Tornquist, CIA, CRMA
Christopher Calvin, CIA
Jiin-Feng Chen, CIA
Andre Domingos
Christina Duquette, CRMA
Marc Eulerich, CIA
Dagmar Flores, CIA, CCSA, CRMA
Anargul Kairulla, CIA
Ayaka Mitsunari
Ahmed Mohammed, CIA
Grace Mubako, CIA
Ruth Doreen Mutebe, CIA
Erika C. Ray, CIA
Brian Tremblay, CIA
Koji Watanabe

Équipe de liaison
Deborah Poulalion –
Directrice de recherche & insights, L'IAI

SPONSORS

PARTENAIRES STRATÉGIQUES DE LA FONDATION

ARABCIIA

AUDITBOARD

Deloitte.

Grant Thornton

The Institute of Internal Auditors
Chicago

The Institute of Internal Auditors

Partenaires de la fondation

African Federation of Institutes of Internal Auditors

Asian Confederation of Institutes of Internal Auditors

Crowe

European Confederation of Institutes of Internal Auditing

Fundación Latinoamericana de Auditores Internos

Partenaires Gold

Larry Harrington
CIA, QIAL, CRMA

Stacey Schabel
CIA

The Institute of Internal Auditors
Houston

The Institute of Internal Auditors
Japan

南京审计大学
NANJING AUDIT UNIVERSITY

The Institute of Internal Auditors
New York

The Institute of Internal Auditors
San Francisco

PARTENAIRES RISK IN FOCUS

IAI – Argentine
IAI – Australie
IAI – Bolivie
IAI – Brésil
IAI – Chili
IAI – Colombie
IAI – Costa Rica
IAI – La République dominicaine
IAI – Équateur
IAI – Salvador
IAI – Ghana
IAI – Guatemala
IAI – Hong Kong
IAI – Indonésie
IAI – Japon
IAI – Kenya
IAI – Malaisie
IAI – Mexique
IAI – Nicaragua
IAI – Panama
IAI – Paraguay
IAI – Pérou
IAI – Les Philippines
IAI – Rwanda
IAI – Singapour
IAI – Afrique du Sud
IAI – Tanzanie
IAI – Ouganda
IAI – Uruguay
IAI – Venezuela

SUR L'IAI

Au sujet de Institute of Internal Auditors (IAI) est une association professionnelle internationale à but non lucratif desservant plus de 235 000 membres à travers le monde et ayant octroyé plus de 190 000 certifications Certified Internal Auditor (CIA) (Auditeur interne certifié) dans le monde entier. Établie en 1941, l'IAI est reconnue à travers le monde comme un leader dans la profession d'audit interne en matière de normes, certifications, éducation, recherche et directives techniques. Pour plus d'informations, veuillez vous rendre sur theiia.org.

Sur l'Internal Audit Foundation

Internal Audit Foundation fournit des renseignements pertinents aux professionnels de l'audit interne et à leurs parties prenantes, tout en promouvant et en faisant progresser la valeur de la profession d'audit interne à travers le monde. Par le biais de l'Academic Fund (Fonds académique), la Fondation soutient le futur de la profession au moyen de subventions visant à soutenir l'éducation en matière d'audit interne dans les institutions d'enseignement supérieur. Pour plus d'informations, veuillez vous rendre sur theiia.org/Foundation.

Avis de non-responsabilité et droits d'auteur

IAI publie ce document à des fins informatives et éducatives. Le présent document n'est pas destiné à fournir des réponses finales à certaines circonstances individuelles et, en conséquence, est uniquement destiné à servir de guide. L'IAI recommande d'obtenir des conseils d'experts indépendants directement liés à toute situation particulière. L'IAI décline toute responsabilité quant à quiconque qui s'appuie uniquement sur ce document.

Internal Audit FOUNDATION

Siège mondial | The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401 | Lake Mary, FL 32746, USA
Téléphone: +1-407-937-1111 | Télécopie: +1-407-937-1101
Site Web: theiia.org