Temps de lecture estimé : 6 minutes

Dans un environnement mondial de plus en plus instable, les organisations font face à des transformations rapides et complexes. Les avancées technologiques avec l'essor de l'intelligence artificielle, les enjeux environnementaux et les tensions géopolitiques redistribuent sans cesse les cartes de l'économie mondiale et renforcent l'exposition des organisations à de nouveaux risques. Les directions d'audit interne s'imposent alors comme des partenaires stratégiques en aidant les organisations à mieux cerner les risques émergents ou en mutation et en les accompagnant dans ce changement.

L'enjeu n'est donc plus seulement de mettre à jour le plan d'audit annuel, mais d'ajuster régulièrement les priorités en fonction de l'évolution du paysage des risques.

C'est pourquoi, nous vous proposons une série de trois articles mettant en lumière les principaux points d'attention que les directions d'audit interne doivent examiner pour anticiper, évaluer et renforcer la maîtrise des risques liés aux enjeux actuels. Le premier article de cette série est consacré aux vulnérabilités technologiques. Dans nos prochaines LAT, vous retrouverez une analyse consacrée aux tensions géopolitiques et aux ruptures des chaînes d'approvisionnement (partie 2), puis un focus sur les enjeux de résilience et de continuité d'activité clôturera cette série (partie 3).

Evaluer les vulnérabilités technologiques

La transformation numérique est devenue un levier stratégique majeur pour permettre aux entreprises de rester compétitives, d'améliorer leurs processus internes et de suivre le rythme rapide des innovations technologiques : intelligence artificielle, cloud computing, blockchain, automatisation robotisée des processus, etc.

Mais cette accélération technologique s'accompagne d'une exposition accrue aux risques, en particulier cyber et en lien avec l'intelligence artificielle.

Les risques cyber

Les organisations sont toujours plus vulnérables aux risques cyber. Leurs services sont massivement ouverts sur Internet, tandis que certains systèmes industriels, souvent anciens, restent essentiels à leur activité et difficiles à sécuriser. **Elles dépendent également davantage d'écosystèmes numériques interconnectés** avec leurs clients, fournisseurs, prestataires, hébergeurs ou plateformes cloud, **susceptibles de gérer des données critiques**.

L'essor du télétravail a aussi accentué certaines failles de sécurité (usage de réseaux personnels ou publics plus permissifs).

En parallèle, les tensions géopolitiques et les rivalités économiques ont transformé le cyberespace en rapport de force numérique.

Les attaques se sont ainsi multipliées et diversifiées : attaques sur les équipements mobiles, déni de service, ransomware, usurpation d'identité, vol de données sensibles, espionnage industriel, etc. Ces incidents, régulièrement médiatisés, concernent désormais toutes les entreprises, quels que soient leur secteur, leur taille ou leur pays.

En 2026, les risques cyber continuent de se durcir et de se complexifier avec l'industrialisation des attaques et l'usage croissant de l'intelligence artificielle. À plus long terme, **les avancées en cryptographie quantique pourraient également transformer en profondeur les pratiques actuelles** en matière de cybersécurité.

L'intelligence artificielle (IA)

L'intelligence artificielle s'impose aujourd'hui comme une stratégie incontournable pour optimiser les coûts ainsi que l'efficacité opérationnelle des organisations. Son développement rapide transforme les modes de travail.

Toutefois, ses résultats peuvent être imparfaits ou difficiles à expliquer. Son déploiement soulève également des risques spécifiques en matière de fiabilité, d'authenticité, d'opacité des algorithmes, de sécurité, de protection des données et de respect des libertés fondamentales.

L'enjeu pour les organisations n'est donc plus seulement d'adopter l'IA, mais **de fiabiliser son usage au travers de principes éthiques et d'un système de gouvernance dédié**. Cette exigence a d'ailleurs été renforcée par l'entrée en vigueur de l'AI Act en août 2024. Ce cadre réglementaire européen, fondé sur les risques, impose aux organisations de sensibiliser ses salariés, de cartographier les systèmes d'IA et d'évaluer leurs risques mais aussi de déployer les mesures techniques et organisationnelles nécessaires.

S'armer contre les vulnérabilités technologiques : le rôle de l'audit interne

Lutter contre les risques cyber

En ce qui concerne les risques cyber, **les directions d'audit interne ont un rôle à jouer pour garantir un socle de confiance**. L'IAA (Institut des Auditeurs Internes) a notamment publié en février 2026 une exigence thématique obligatoire pour normer les missions d'audit interne en matière d'évaluation de la cybersécurité au sein des organisations.

Le plan d'audit cyber doit ainsi couvrir trois dimensions clés.

- ✓ Une gouvernance claire et alignée avec la stratégie globale de l'organisation.
- ✓ Une gestion des risques robuste et suffisamment agile pour anticiper et traiter rapidement les menaces émergentes, qui intègre des dispositifs éprouvés (sensibilisation de l'ensemble des salariés de l'organisation, tests réguliers d'intrusion ou encore un dispositif éprouvé de réponses aux incidents cyber).
- ✓ Des contrôles opérationnels efficaces, y compris lorsqu'ils sont confiés à des prestataires.

Le **référentiel MAGNum 2026**, publié par l'IFACI, le CIGREF et ISACA France, peut constituer un appui utile pour apprécier la maturité de la gouvernance numérique et structurer le dialogue avec les différentes parties prenantes.

Lutter contre les déviances liées à l'IA

En ce qui concerne l'utilisation de l'IA au sein des organisations, les directions d'audit interne ont également pour mission d'apprécier la maturité du dispositif de gouvernance dédié à l'IA et d'accompagner la modernisation tout au long du cycle de vie des systèmes d'IA (notamment en matière d'évaluation des risques et de contrôles). Elles s'assurent aussi du respect de la réglementation en vigueur (notamment au RGPD). Elles devront pour cela faire évoluer leurs compétences et être capables de comprendre les aspects techniques, éthiques et réglementaires liés à l'IA.

Pour conclure

Les organes de gouvernance attendent des directions de l'audit interne qu'elles s'emparent des problématiques émergentes sans attendre que les risques se matérialisent. Les directions d'audit interne doivent dépasser leur rôle traditionnel d'assurance et s'imposer comme des partenaires de confiance pour sécuriser la transformation des organisations en renforçant la gouvernance, la maîtrise des risques et l'efficacité des contrôles.