
XL Insurance
Construire une IA résiliente
Gérer les risques liés à l'IA grâce à la gouvernance, à la sécurité et à la résilience
Produit en partenariat avec S-RM

Sommaire

Préface

La confiance est au cœur de toute entreprise prospère. Elle renforce les relations, permet l'innovation et donne aux organisations l'assurance nécessaire pour s'adapter au changement. Aujourd'hui, les organisations accordent une confiance croissante à l'intelligence artificielle. Pourtant, la gouvernance nécessaire pour l'accompagner peine à suivre le rythme.

L'IA a largement dépassé le stade des projets pilotes isolés ou des simples outils de productivité. Elle est en passe de devenir une composante essentielle des systèmes et processus sur lesquels les organisations s'appuient au quotidien pour prendre des décisions, servir leurs clients, améliorer leur productivité et stimuler l'innovation. Le rythme soutenu des avancées technologiques a ouvert des perspectives majeures, mais a également fait émerger une nouvelle catégorie de risques pour les entreprises.

À mesure que l'IA s'intègre aux fonctions critiques de l'entreprise, la gouvernance des données, la protection de l'intégrité des modèles d'IA, les risques liés aux tiers et l'évolution de la réglementation deviennent de plus en plus difficiles à gérer. Cette évolution touche tous les secteurs, et l'IA est désormais considérée comme l'un des défis les plus importants auxquels les entreprises sont confrontées à l'échelle mondiale.

Alors que les organisations continuent d'accroître leurs investissements dans les capacités offertes par l'IA, il est évident que les décisions prises aujourd'hui façonneront la résilience, la confiance des clients et le positionnement concurrentiel pour les années à venir.

Pour les conseils d'administration et les équipes dirigeantes, la sécurité de l'IA doit être envisagée comme bien plus qu'un simple sujet technologique. Elle exige un leadership fort, des responsabilités claires, une gouvernance robuste et une attention toute particulière portée à la résilience de l'entreprise. Les organisations qui tireront le plus de valeur de leurs investissements dans l'IA seront celles qui savent où elle est utilisée, qui instaurent une supervision claire tout au long de son cycle de vie et qui mettent en place les garde-fous nécessaires dès le début.

Ce rapport analyse l'évolution du paysage des risques liés à l'IA et présente des mesures concrètes permettant aux organisations de l'adopter dès aujourd'hui en toute confiance. S'appuyant sur les analyses d'AXA XL et de S RM, ainsi que sur des études sectorielles de référence, il explique comment les entreprises peuvent déployer l'IA à grande échelle de manière fiable et responsable.

Jonathan Salter
Global Head of Risk Consulting

Rebiah Bardot-Girard
Head of Cyber Risk Consulting Services

Résumé exécutif

La sécurité de l'IA entre dans une nouvelle phase. Les enjeux dépassent désormais largement les modèles pris isolément pour englober les systèmes, la gouvernance et les interdépendances qui façonnent le déploiement de l'IA dans les entreprises. Parallèlement, les progrès rapides de l'IA agentique, l'évolution de la réglementation et la sophistication croissante des menaces cyber influencent la manière dont les organisations appréhendent les risques.

Cinq évolutions en particulier déterminent désormais les priorités des dirigeants d'entreprise :

À retenir

L'IA crée de nouvelles opportunités tout en générant de nouvelles formes de risques. Ceux qui considèrent la gouvernance de l'IA comme une priorité stratégique pour l'entreprise, plutôt que comme un simple exercice de conformité, seront les mieux placés pour permettre à leur organisation de déployer l'IA de manière sécurisée, de s'adapter à la réglementation et d'en tirer une valeur à long terme.

De nouvelles catégories de risques cyber émergent

L'IA est, dans une certaine mesure, une arme à double tranchant pour les équipes de cybersécurité. D'un côté, elle contribue à renforcer les défenses, mais elle fournit simultanément aux attaquants de nouvelles capacités. Les entreprises sont également confrontées à des risques propres à l'IA elle-même : fuite de données, modèles empoisonnés ou manipulés, attaques par injection de prompts, réponses de modèles que les systèmes en aval acceptent sans validation, systèmes de recherche et de récupération d'informations qui exposent des données au-delà des droits habituels d'un utilisateur, et sécurité d'agents autonomes agissant avec leurs propres identifiants. Ces risques ne sont plus théoriques. Des voix et vidéos synthétiques sont déjà utilisées pour autoriser des paiements frauduleux, et certaines organisations ont été tenues responsables de déclarations formulées à leurs clients par leurs propres systèmes d'IA.

La réglementation sur l'IA s'accélère à l'échelle mondiale

Les gouvernements et les régulateurs s'emploient à établir rapidement des attentes concrètes en matière de développement et d'utilisation responsables. Même si les approches diffèrent selon les régions, un constat s'impose partout : les entreprises devront démontrer qu'elles utilisent l'IA de manière responsable.

La gouvernance devient un avantage concurrentiel

Les organisations qui établissent clairement les responsabilités et disposent d'une supervision solide ont bien plus de chances de déployer ces technologies avec succès et de suivre l'évolution des risques, renforçant ainsi la confiance de leurs publics. La supervision doit également couvrir les usages de l'IA dont elles n'ont pas connaissance. L'usage par les employés d'outils publics d'IA, ainsi que l'activation de fonctionnalités IA au sein de logiciels existants, représentent aujourd'hui deux des sources d'exposition les plus répandues.

L'IA doit être gérée sur l'ensemble de son cycle de vie

La gestion des risques liés à l'IA va au-delà de la sécurisation de modèles isolés. Une visibilité sur l'ensemble du cycle de vie, depuis la collecte des données et le développement des modèles jusqu'à leur déploiement et leur supervision, sera indispensable. Cela inclut les fournisseurs tiers, car les écosystèmes d'IA sont interconnectés et la responsabilité ne peut être déléguée. La gestion du cycle de vie implique aussi la capacité de reconstituer les événements. Sans conserver de traces des prompts, des résultats et des appels aux outils, les incidents impliquant des systèmes d'IA ne peuvent pas être analysés avec le même degré de fiabilité que les incidents informatiques classiques.

Clarifier l'atténuation et l'assurance des risques liés à l'IA

Les entreprises qui adoptent l'IA auront besoin d'aide pour comprendre les vulnérabilités qu'elles peuvent involontairement créer. La gestion des risques et l'assurance jouent un rôle important pour aider les entreprises à mieux cerner leur exposition, renforcer leur résilience avant qu'un incident ne survienne et les soutenir dans une reprise d'activité efficace lorsque la perturbation ne peut être évitée. Il convient également de clarifier la manière dont les pertes liées à l'IA s'articulent avec les garanties existantes. Chacun de ces scénarios peut relever de garanties différentes : un paiement frauduleux autorisé au moyen d'un appel vidéo synthétique, un résultat d'IA défectueux causant une perte chez un tiers ou une intrusion permise par un agent d'IA.

L'intégration de l'IA dans l'entreprise

Dans tous les secteurs, les organisations intègrent l'IA au cœur de leurs processus, l'utilisant pour améliorer les interactions avec les clients, rationaliser les opérations, analyser les données et faciliter la prise de décision.

La dernière enquête « State of AI » de McKinsey révèle que 88 % des organisations déclarent désormais utiliser régulièrement l'IA dans au moins une fonction métier, contre 78 % un an plus tôt. L'IA est donc devenue un outil courant dans les organisations.[1]

L'IA devient également plus autonome, les entreprises délaissant progressivement les simples outils de génération de contenu au profit de systèmes capables de rechercher des informations, d'interagir avec d'autres applications et d'exécuter des actions avec une intervention humaine limitée. Cette évolution peut apporter des gains d'efficacité significatifs, mais elle accroît aussi les conséquences potentielles des défaillances de sécurité et des erreurs opérationnelles.

1. McKinsey & Company, The State of AI, 2026

L'IA étant désormais essentielle à de nombreuses opérations, les effets d'une défaillance peuvent se propager rapidement d'un système à l'autre et être difficiles à détecter avant que leurs conséquences ne se manifestent. La réussite de la prochaine phase d'adoption de l'IA dépendra de la capacité des organisations à gérer l'écosystème plus large qui entoure leurs modèles. Il devient fondamental de comprendre où l'IA est utilisée, comment elle interagit avec les processus métier et qui est responsable de ses résultats afin de renforcer la résilience de son déploiement. À mesure que les entreprises dépendent davantage des écosystèmes d'IA, de nouvelles interconnexions se créent entre les personnes, les technologies et les prestataires tiers. Cette transformation accroît à la fois l'ampleur des opportunités et les conséquences potentielles des défaillances.

88%

des organisations utilisent régulièrement l'IA dans au moins une fonction métier. Selon McKinsey, 2026.

À retenir

L'IA s'intègre au tissu opérationnel des organisations modernes, au sein d'écosystèmes technologiques de plus en plus interconnectés. Les entreprises doivent rapidement composer avec un niveau de complexité que peu de modèles de gouvernance ont été conçus pour gérer. La sécurité doit désormais aller au-delà de la protection des modèles isolés pour englober les données, les systèmes, les fournisseurs et les processus métier qui permettent à l'IA de fonctionner de manière sûre à grande échelle.

Le paysage des risques liés à l'IA

Les organisations sont confrontées à une amplification des risques cyber traditionnels. Ces risques ne sont pas de simples problèmes techniques isolés. Ils peuvent affecter simultanément la gouvernance, la sécurité et la résilience. Par ailleurs, les défis existants autour de l'identité, des données, des chaînes d'approvisionnement et de la résilience opérationnelle deviennent de plus en plus complexes.

Ces risques ne sont pas nouveaux. Le vol de données, les menaces internes et les vulnérabilités logicielles sont des défis de longue date. Ce que l'IA change, c'est l'échelle et la complexité. Les systèmes actuels traitent davantage d'informations, interagissent avec davantage d'applications et prennent ou influencent plus de décisions, avec un niveau d'autonomie jamais atteint.

Les entreprises prennent progressivement conscience de la nécessité d'anticiper ces nouveaux risques. Le dernier rapport « Global Cybersecurity Outlook » du World Economic Forum révèle que 64 % des organisations disposent aujourd'hui de processus permettant d'évaluer la sécurité des outils d'IA avant leur déploiement [2], contre 37 % l'année précédente. Pour les dirigeants, la conclusion est claire : la sécurité de l'IA doit être intégrée dès le départ plutôt qu'après la mise en production, et envisagée dans une perspective de gouvernance globale, plutôt que comme une question purement technique et circonscrite.

La première étape consiste à comprendre comment le paysage des risques liés à l'IA évolue, où de nouvelles vulnérabilités apparaissent et ce qu'elles signifient pour l'entreprise.

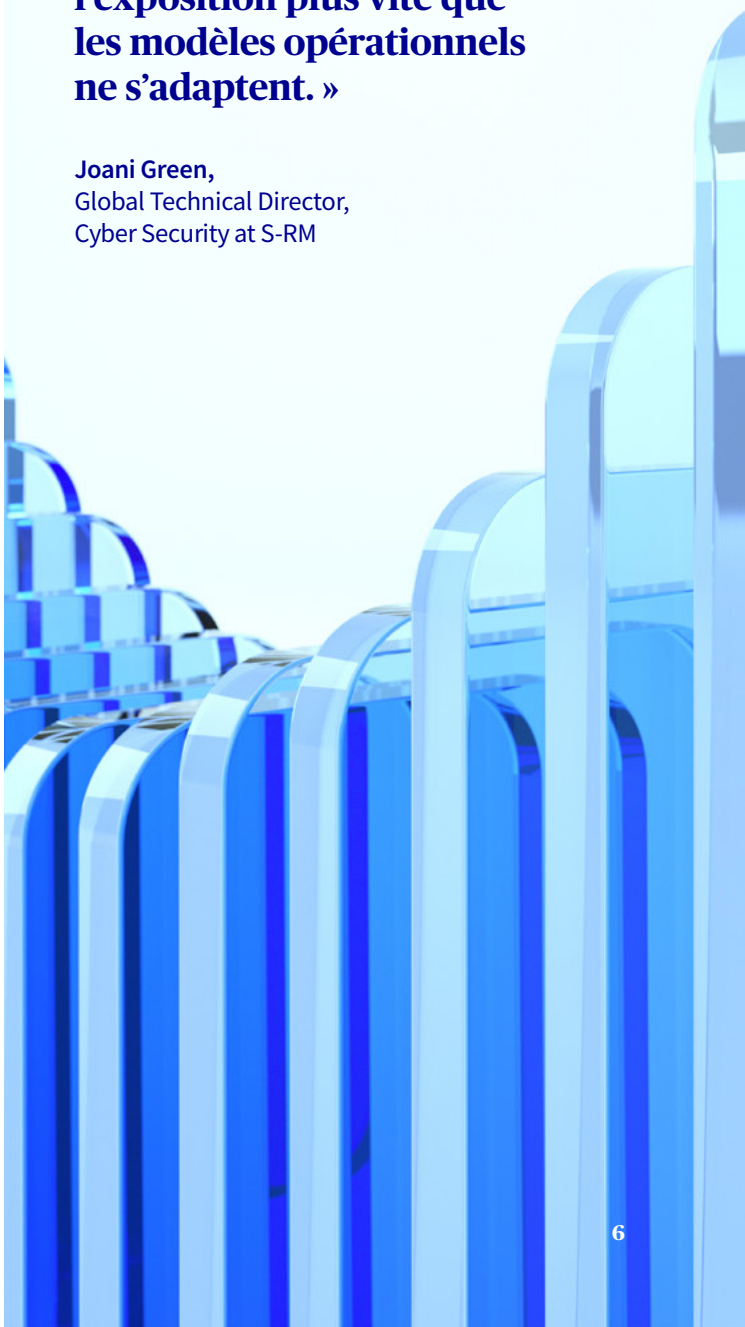
[2] World Economic Forum, Global Cybersecurity Outlook, 2026

64%

des organisations disposent aujourd'hui de processus permettant d'évaluer la sécurité des outils d'IA avant leur déploiement

« D'après notre expérience auprès des organisations confrontées à des incidents cyber et cherchant à renforcer leur résilience, un constat s'impose de plus en plus clairement : le risque lié à l'IA ne se manifeste pas isolément. Il se superpose à des faiblesses existantes en matière de gestion des identités, de gouvernance des données, de surveillance des fournisseurs et de préparation aux incidents. Pour beaucoup d'organisations, l'IA accélère l'exposition plus vite que les modèles opérationnels ne s'adaptent. »

Joani Green,
Global Technical Director,
Cyber Security at S-RM



Lutter contre la fuite de données et les accès non autorisés

Les systèmes d'IA reposent sur de grands volumes de données pour produire des résultats précis et utilisent souvent des informations commercialement sensibles ou relevant de la propriété intellectuelle. À mesure que l'IA s'intègre davantage au quotidien, ces données deviennent encore plus précieuses et, dans de nombreux cas, plus largement accessibles que jamais.

Sans gouvernance solide, des informations sensibles peuvent facilement se retrouver dans les prompts, les réponses ou des applications tierces, générant des risques qui dépassent largement la cybersécurité. À mesure qu'un nombre croissant de systèmes et d'applications accèdent à des données sensibles par l'intermédiaire de l'IA, il devient d'autant plus crucial de contrôler qui, ou quel système, peut accéder à ces informations. Les attaquants ciblent aussi les identités et les privilèges d'accès qui ouvrent la voie vers ces données.

L'Index « X Force Threat Intelligence » 2025 d'IBM montre que plus de 30 % des incidents analysés impliquaient le vol ou l'utilisation abusive d'identifiants de connexion, traduisant une évolution de l'exploitation traditionnelle de failles logicielles vers des attaques centrées sur l'identité. [3]

Les entreprises ont plus que jamais besoin d'une compréhension très claire de l'utilisation des données, de la façon dont elles circulent entre les systèmes et de qui peut y accéder. Cette visibilité est essentielle pour gérer les risques, en particulier lorsque des données sensibles ou personnelles sont concernées. Du point de vue de l'assurance, les organisations capables de démontrer une gouvernance solide des données, des contrôles d'accès robustes et une supervision claire des systèmes d'IA sont bien mieux placées pour réduire leur exposition.

Pour les dirigeants, la protection des données n'est plus seulement une question de sécurité de l'information. Elle devient fondamentale pour maintenir la confiance des clients et garantir la fiabilité des décisions éclairées ou influencées par l'IA.

À retenir

Une gouvernance efficace de l'IA commence par une compréhension claire des données auxquelles les systèmes peuvent accéder, de leur emplacement et de la manière dont elles sont protégées, quel que soit le contexte dans lequel elles sont utilisées.

[3] IBM, X-Force Threat Intelligence Index, 2025

Empoisonnement des données

Dans les systèmes d'IA, les données sont l'un des éléments centraux du modèle. L'empoisonnement des données intervient lors de la phase d'entraînement, lorsque des acteurs malveillants injectent délibérément des éléments corrompus dans les données d'entraînement afin d'orienter les résultats et d'influencer le comportement du modèle. L'objectif est de dégrader les performances globales du modèle ou d'y introduire une porte dérobée (« backdoor »), susceptible de déclencher un comportement malveillant dans certaines conditions.

Lorsque les résultats d'un système d'IA sont faussés dès l'entraînement, la manipulation est souvent difficile à détecter après le déploiement, et sa correction peut nécessiter un réentraînement complet du modèle à partir de données fiables. Les conséquences ne se limitent pas aux performances : elles érodent la confiance, fragilisent la sécurité et la gouvernance, et peuvent introduire des risques réglementaires ou métier.

Les organisations doivent assurer une traçabilité rigoureuse de la provenance des données d'IA dès les premières étapes du projet et définir des techniques d'entraînement robustes. Elles doivent également superviser en continu l'ensemble du processus d'entraînement afin de détecter rapidement tout indice de manipulation, tout en prévoyant des étapes de contrôle humain.

À retenir

Intégrer de bonnes pratiques de gouvernance des données dès la première étape d'un projet d'IA et les adapter, si nécessaire, tout au long de son cycle de vie.

Attaques par injection de prompts et manipulations adversariales

La capacité de manipuler les instructions reçues par les systèmes d'IA au moyen de prompts, ou de tromper délibérément le modèle pour obtenir de mauvaises prédictions grâce à des données d'entrée malveillantes, telles que des images, des textes ou des contenus audio, constitue une autre source de risque à laquelle les entreprises doivent se préparer. Influencer le comportement d'un système ou contourner ses garde-fous afin de produire des résultats involontaires ou nuisibles peut avoir de lourdes conséquences.

Lorsque les réponses générées par l'IA sont manipulées, les conséquences peuvent aller de la divulgation d'informations confidentielles à l'influence sur des décisions métier, en passant par la perturbation de services destinés aux clients, en particulier lorsque l'IA est intégrée aux opérations quotidiennes.

Les organisations doivent s'assurer que les tests de sécurité des données et des systèmes, la supervision et le contrôle humain évoluent au même rythme que l'utilisation des technologies intégrant l'IA. Autrement dit, il faut traiter les systèmes d'IA avec la même discipline que n'importe quel autre système critique.

Parce que l'IA joue un rôle plus actif dans les interactions avec les clients, les organisations ne peuvent plus se permettre de traiter l'injection de prompts comme une vulnérabilité purement technique. Elle constitue désormais un risque à l'échelle de l'entreprise, qui nécessite une supervision constante.

À retenir

Les résultats produits par l'IA doivent être vérifiés, supervisés et encadrés par une gouvernance appropriée, plutôt que présumés exacts ou sécurisés par défaut.

Hallucinations et réponses non fiables

L'IA générative est capable de choses remarquables, mais peut produire avec assurance des réponses erronées. Les hallucinations résultent de lacunes dans les données d'entraînement, de prompts ambigus ou de limites propres au modèle.

Selon l'édition 2026 de l'AI Index de l'Université de Stanford, les taux d'hallucination observés parmi 26 grands modèles d'IA varient de 22 % à 94 %. [4]

Un résultat erroné peut sembler mineur lorsqu'il est considéré isolément. Mais lorsque l'IA contribue à façonner les décisions métier, à assister les clients ou à piloter des processus opérationnels, les enjeux sont nettement plus élevés. Les erreurs peuvent se propager rapidement, entraînant une surveillance réglementaire accrue, des pertes financières et une atteinte durable à la confiance.

[4] Stanford University, AI Index Report, 2026

Les organisations doivent mettre en place des processus de validation réguliers, plutôt que des contrôles ponctuels, et déterminer où une supervision humaine est nécessaire.

Les entreprises doivent pouvoir faire confiance non seulement aux résultats produits par l'IA, mais aussi à leur capacité de déterminer quand ces résultats sont fiables et quand le jugement humain doit prévaloir.

À retenir

La confiance dans l'IA dépend de la vérification de ses résultats, et non de la présomption de leur exactitude.

Manipulation et vol de modèles

Pour de nombreuses entreprises, les modèles d'IA constituent désormais des actifs stratégiques, reflétant des investissements importants et intégrant un savoir-faire propriétaire précieux. À mesure que leur importance croît, ils attirent davantage les cybercriminels.

La protection des modèles d'IA doit devenir aussi stratégique que celle des données clients ou des infrastructures critiques. Lorsque des modèles d'IA sont manipulés, l'intégrité des processus pilotés par l'IA peut être compromise. S'ils sont volés, les attaquants peuvent accéder à une propriété intellectuelle de valeur ou reproduire des capacités dont le développement a pris des années. Cela peut gravement compromettre la confiance dans les services intégrant l'IA et porter durablement atteinte à l'innovation.

Leur protection ne peut se limiter à de simples contrôles techniques. Les organisations doivent comprendre où les modèles sont déployés, qui peut y accéder, comment les changements sont gérés et quels garde-fous existent pour détecter toute activité non autorisée.

À retenir

Les modèles d'IA doivent être protégés et gouvernés comme des actifs critiques de l'entreprise.

Lutter contre l'IA fantôme (« shadow AI »)

L'IA fantôme désigne les situations dans lesquelles des employés ou des équipes métier utilisent des outils ou services d'IA qui n'ont pas fait l'objet de revues formelles de sécurité, de confidentialité et de gouvernance. Ces outils peuvent traiter des données sensibles ou interagir avec les systèmes de l'entreprise, en contournant souvent les processus d'approvisionnement et les évaluations des risques.

Les risques incluent les fuites ou les exfiltrations de données, ainsi que l'introduction de configurations insuffisamment sécurisées ou de portes dérobées qui élargissent la surface d'attaque de l'organisation. Sur le plan opérationnel, l'IA fantôme peut créer des flux de données non maîtrisés, des problèmes de licences et de coûts, des résultats incohérents et des difficultés d'audit.

Sur le plan stratégique, elle fragilise la gestion des risques, augmente la dépendance aux fournisseurs et complique la réponse aux incidents ainsi que la continuité d'activité.

Pour y répondre, les entreprises devraient bloquer par défaut les outils non autorisés et instaurer une politique claire ainsi qu'un processus d'approbation pour les outils d'IA, tout en appliquant les principes de classification des données et du moindre privilège. La formation régulière des employés et l'évaluation périodique de la surface d'attaque sont également essentielles pour éviter ces situations.

À retenir

La maîtrise des usages non autorisés de l'IA est devenue indispensable.

« Les risques les plus difficiles ne sont pas toujours les plus visibles. Les entreprises peuvent avoir une gouvernance formelle sur les programmes stratégiques d'IA, alors que des usages non gérés se poursuivent au moyen d'outils publics, de fonctionnalités logicielles intégrées ou de services tiers. Cela crée un décalage entre la perception du contrôle et l'exposition réelle. Combler ce fossé commence par un inventaire pratique des usages de l'IA, des données auxquelles elle peut accéder et des actions qu'elle peut prendre ou influencer. »

Joani Green,
Global Technical Director, Cyber Security at S-RM

Dépendance à des modèles non vérifiés ou à des modèles tiers

Le recours à des sous-traitants ou à des fournisseurs externes de modèles d'IA soulève des enjeux en matière de chaîne d'approvisionnement et de gouvernance. Une visibilité limitée sur la façon dont le modèle a été entraîné, les données utilisées et la manière dont les mises à jour sont gérées peut accroître le risque de comportements indésirables et de non-conformité aux politiques internes.

Comme pour tout autre fournisseur informatique, la dépendance à un prestataire d'IA crée des points de dépendance critiques en cas de panne, de modification des orientations stratégiques ou de changement de tarifs, et peut limiter l'alignement stratégique avec les normes internes.

En outre, des modèles non vérifiés ou mal évalués peuvent exposer les organisations à de potentielles portes dérobées ou à des comportements dangereux.

Les divergences en matière de politiques, de réglementation ou d'éthique constituent une autre préoccupation majeure, en particulier lorsque les modèles dérivent après leur déploiement ou sont mis à jour sans tests approfondis. Les ambiguïtés liées aux licences et le manque de transparence sur les données d'entraînement compliquent aussi la conformité et les audits.

Plutôt que de considérer les modèles externes comme sûrs par défaut, une gouvernance robuste et un audit préalable doivent s'appliquer à l'ensemble des modèles et des données. Une provenance claire et la traçabilité des activités doivent être exigées, des validations de sécurité et fonctionnelles doivent être imposées avant le déploiement, et des protections contractuelles fortes (niveau de service, clauses de transparence, obligations de divulgation des mises à jour) doivent être définies.

À retenir

Les fournisseurs d'IA doivent être traités comme des tiers critiques. Le fournisseur et le modèle d'IA doivent tous deux faire l'objet de contrôles et d'audits préalables.

Agents d'IA autonomes

Au-delà de la simple génération de contenu ou de réponses à des prompts, les systèmes d'IA agentiques sont désormais capables de planifier des tâches, d'interagir avec des applications et d'exécuter des actions avec une intervention humaine limitée. Leur potentiel est considérable, puisqu'ils permettent aux entreprises d'automatiser des processus complexes. Toutefois, ce niveau accru d'autonomie soulève de nouveaux défis de gouvernance.

Les systèmes d'IA nécessitent des autorisations clairement définies et des garde-fous appropriés afin de fonctionner dans des limites clairement définies. Sans supervision efficace, ils risquent d'accéder à des données inappropriées ou d'interagir avec des systèmes connectés d'une manière susceptible de créer de nouvelles vulnérabilités.

L'enquête McKinsey a montré que 23 % des organisations industrialisent déjà l'IA agentique dans au moins une fonction métier, tandis que 39 % supplémentaires expérimentent des agents d'IA. [5]

Ce rythme d'adoption souligne la rapidité avec laquelle ces systèmes s'intègrent aux opérations quotidiennes. Les entreprises doivent concilier les bénéfices de l'automatisation avec un niveau approprié de responsabilité et de contrôle humain. Plus les organisations accordent d'autonomie à l'IA, plus il est crucial de définir clairement qui en assume la responsabilité.

À retenir

Plus les entreprises accordent d'autonomie à l'IA, plus elles ont besoin d'une gouvernance efficace, d'autorisations clairement définies et d'une véritable supervision humaine.

Pris isolément, la fuite et l'empoisonnement des données, l'IA fantôme, l'injection de prompts, la manipulation et le vol de modèles, les hallucinations et les agents d'IA autonomes peuvent sembler constituer des défis techniques distincts. Mais, ensemble, ils témoignent d'une évolution beaucoup plus large du paysage des risques en entreprise : la nécessité d'une gouvernance couvrant l'ensemble de l'écosystème de l'IA, plutôt que d'un traitement isolé de chaque risque.

Cependant, la compréhension des risques n'est qu'une partie du défi. À mesure que l'adoption s'accélère, les organisations doivent aussi évoluer dans un environnement réglementaire qui redéfinit les attentes. Gérer les risques exige désormais une approche plus intégrée que jamais, tenant compte de l'interdépendance entre la technologie, les personnes, les processus et les fournisseurs tiers.

[5] McKinsey & Company, The State of AI 2026

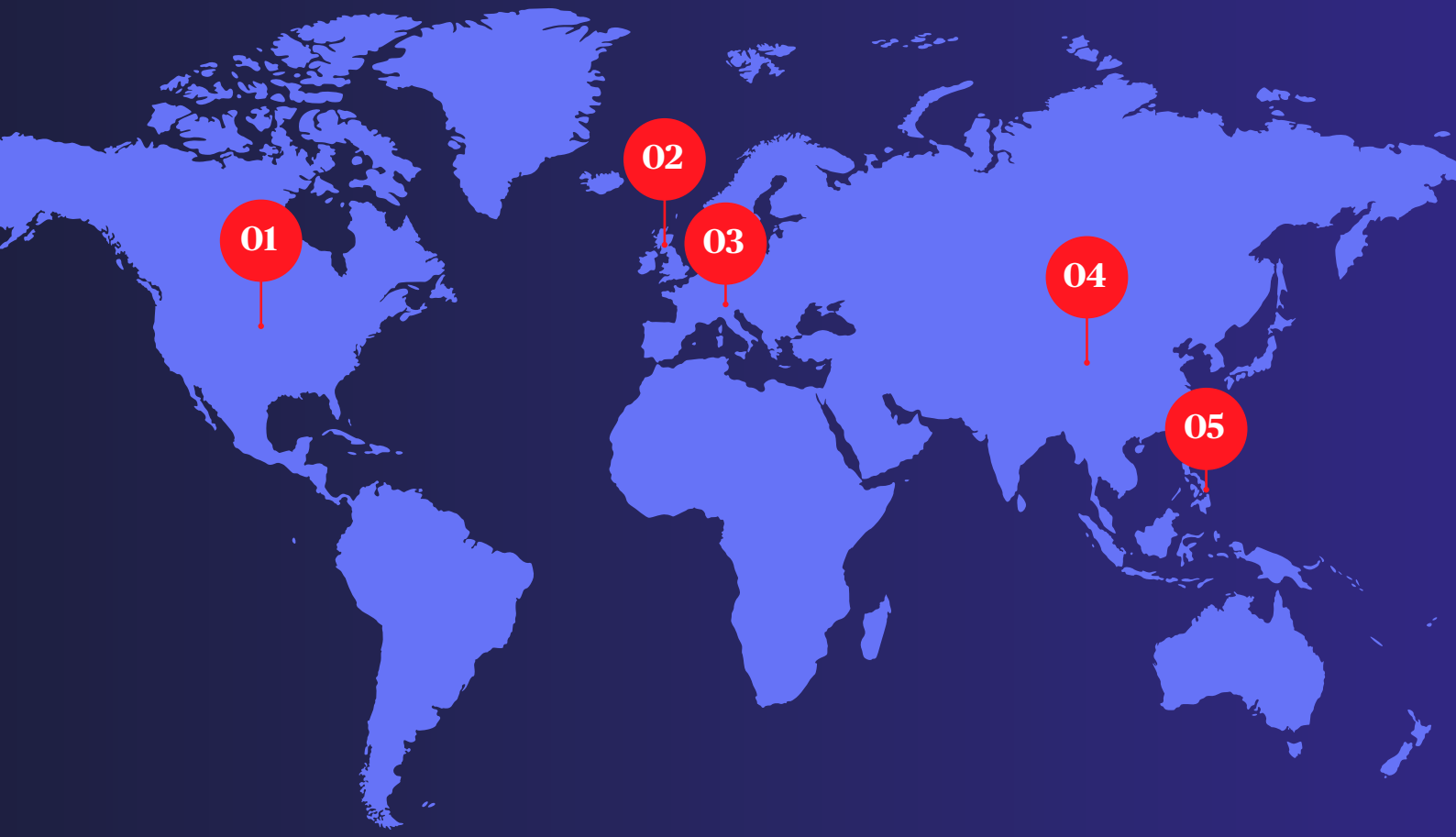
Naviguer dans la réglementation actuelle et future

L'environnement réglementaire mondial de l'IA évolue rapidement, tandis que les décideurs s'attachent à définir des garde-fous concrets qui encadreront cette technologie. L'OCDE [6] a souligné cette évolution, notant que les gouvernements vont au-delà des grandes orientations stratégiques sur l'IA pour élaborer des règles plus précises et renforcer la responsabilité, afin de favoriser une adoption sûre.

Si les approches diffèrent, une tendance générale se dessine. Il est de plus en plus attendu des organisations qu'elles sachent où l'IA est déployée, qu'elles mettent en place une gouvernance appropriée et qu'elles démontrent que les responsabilités sont clairement établies tout au long du cycle de vie.

Plutôt que de réagir à chaque nouvelle réglementation isolément, les organisations devraient s'attacher à mettre en place des cadres de gouvernance suffisamment flexibles pour s'adapter à l'évolution des exigences.

[6] OECD, Governing with Artificial Intelligence



Évolutions réglementaires mondiales

Les entreprises présentes à l'international devront composer avec une mosaïque de réglementations sur l'IA. Bien que de nombreux gouvernements partagent des objectifs similaires, le rythme, la portée et les priorités réglementaires varient sensiblement d'une région à l'autre :

01 **États Unis** Le pays fait face à un paysage réglementaire plus fragmenté et incertain, avec une politique en matière d'IA en constante évolution au niveau fédéral comme au niveau des États. Les différences entre ces approches, ainsi que les incertitudes entourant l'articulation des exigences fédérales et locales, obligent les entreprises à se préparer à un environnement susceptible de continuer à évoluer rapidement.

02 **Royaume Uni** Le Royaume-Uni a adopté une approche fondée sur des principes, visant à encourager l'innovation tout en appliquant les cadres réglementaires existants à l'IA. L'accent est mis sur la démonstration d'une gouvernance responsable, transparente et clairement attribuée, plutôt que sur la création de règles entièrement nouvelles.

03 **Europe** L'Union européenne continue de donner le ton avec le règlement européen sur l'IA (AI Act), qui classe les systèmes d'IA selon les risques potentiels pour les individus, notamment pour leur sécurité et leurs droits fondamentaux. Les systèmes à haut risque sont soumis à des exigences plus strictes en matière de supervision, de transparence et de responsabilité. Bien que la législation s'applique au sein de l'UE, son influence s'étend déjà au-delà, incitant les entreprises à renforcer la gouvernance de l'IA dans leurs opérations internationales.

04 **Chine** La Chine a développé son propre cadre réglementaire pour l'IA, avec des exigences couvrant des domaines tels que les services d'IA générative, les algorithmes, les données et les contenus. Son approche évolue au rythme de la forte croissance du secteur. Les évolutions observées en Chine revêtent donc une importance croissante pour les entreprises présentes à l'international ou dépendantes de technologies d'IA et de fournisseurs chinois.

05 **Région Asie-Pacifique au sens large** Les approches réglementaires continuent de se structurer à des rythmes différents, tout en faisant apparaître des thèmes communs liés à l'IA responsable, à la gestion sécurisée des données et à une supervision efficace. Les organisations présentes à l'international auront besoin d'une approche capable de s'adapter à des exigences variées, à mesure que le paysage réglementaire se structure.

Ce que la réglementation sur l'IA implique pour les entreprises

Même si les approches réglementaires varient, elles convergent vers des attentes similaires.
Les organisations doivent savoir où elles utilisent l'IA, identifier les systèmes à haut risque, définir clairement les responsabilités et conserver des traces précises de l'utilisation de l'IA sur l'ensemble de son cycle de vie.

L'explicabilité et la responsabilité deviennent aussi importantes que les performances techniques, notamment lorsque l'IA influence des décisions qui affectent les clients, les employés ou les opérations critiques. Pour les dirigeants, cela renforce l'idée que la gouvernance de l'IA est une responsabilité à l'échelle de l'entreprise.

La conformité comme levier de création de valeur

Les organisations peuvent percevoir la réglementation comme une contrainte à l'innovation, mais la réalité est qu'une gouvernance efficace peut devenir un avantage concurrentiel.

Les dernières recherches « State of AI in the Enterprise » de Deloitte [7] révèlent que seule une organisation sur cinq dispose d'un modèle de gouvernance mature pour les agents d'IA autonomes, ce qui offre une opportunité pour les entreprises qui instaurent une gouvernance robuste très tôt.

Les organisations capables de démontrer que les responsabilités sont clairement établies, que leur gouvernance est cohérente et que leurs pratiques sont transparentes seront mieux placées pour répondre aux nouvelles exigences réglementaires et gagner la confiance de leurs clients et partenaires.

[7] Deloitte, State of AI in the Enterprise

« L'IA modifie également les preuves dont les organisations ont besoin après un incident. Les journaux d'activité traditionnels peuvent ne pas suffire pour comprendre ce qui s'est passé, en particulier lorsque des prompts, des réponses, le comportement du modèle, les sources utilisées pour la recherche et la récupération d'informations ou les actions des agents sont en jeu.

Les organisations devraient réfléchir aux informations nécessaires pour reconstituer un événement lié à l'IA, démontrer leur responsabilité et soutenir les démarches juridiques, réglementaires ou assurantielles. »

Joani Green,
Global Technical Director,
Cyber Security at S-RM

Savoir ce que les régulateurs attendent est une chose, mais se doter des capacités organisationnelles nécessaires pour répondre durablement à ces attentes en est une autre. C'est là que les cadres de gouvernance deviennent précieux, non seulement comme exercice de conformité, mais comme outil pratique pour ancrer la résilience dans les opérations quotidiennes. Les organisations qui investissent dès aujourd'hui dans cette démarche seront mieux placées pour répondre aux futures exigences réglementaires.

Du risque à la résilience

À mesure que cette technologie se généralise, les organisations auront besoin de moyens pragmatiques pour gérer les risques de façon cohérente, alors même que les systèmes évoluent. Cela implique d'aller au-delà des contrôles techniques isolés et d'adopter des modèles de gouvernance qui rassemblent différentes équipes autour d'une approche commune.

Aucun référentiel unique ne peut répondre à l'ensemble des défis associés à l'IA. Toutefois, des normes et référentiels reconnus, tels que le NIST AI Risk Management Framework, l'ISO/IEC 42001, le Top 10 OWASP pour les applications reposant sur de grands modèles de langage [8] et le Top 10 OWASP pour les applications agentiques [9], offrent une base solide.

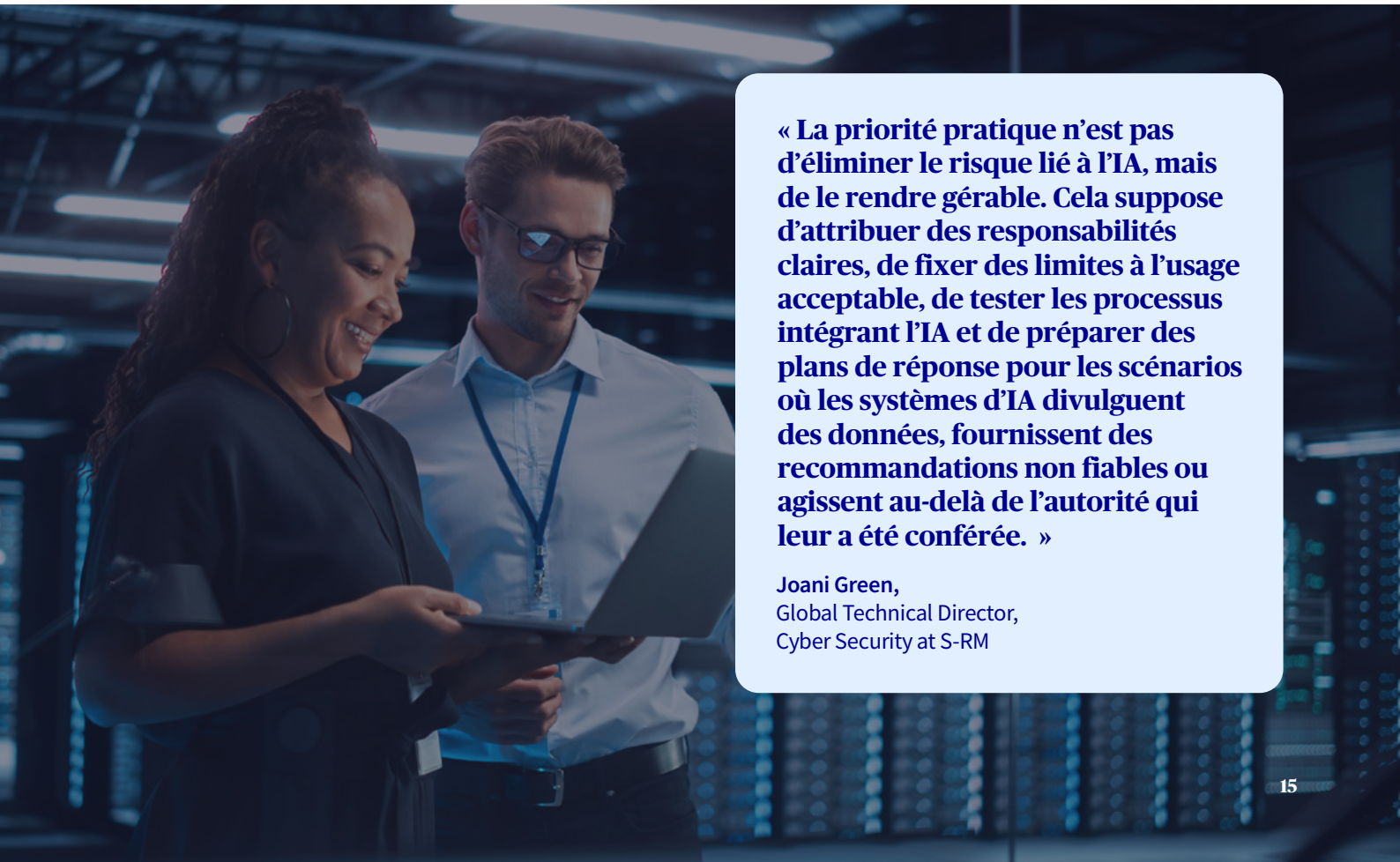
Plutôt que de prescrire des contrôles techniques spécifiques, ces référentiels offrent aux organisations un moyen cohérent d'évaluer les risques, d'attribuer les responsabilités et de gouverner l'IA. Ensemble, ils encouragent une approche plus uniforme pour identifier les usages de l'IA à haut risque, gérer les dépendances aux tiers, superviser les performances des systèmes d'IA et réagir aux incidents à mesure que les systèmes évoluent.

En définitive, la résilience dépend moins de l'adoption d'un cadre particulier que de l'intégration d'une bonne gouvernance dans les décisions quotidiennes. Maintenir une visibilité sur les systèmes d'IA et suivre en continu leurs performances permettent de garantir que les entreprises sont prêtes à gérer les risques émergents tout en continuant d'innover en toute confiance.

Perspectives

Les cadres de gouvernance fixent un cap, mais ils ne créent de valeur que lorsqu'ils se traduisent dans les pratiques quotidiennes. Le prochain défi pour les entreprises sera de transformer ces principes en pratiques concrètes pour la conception, le développement, le déploiement et la gestion des systèmes d'IA. La sécurité et la résilience doivent faire partie intégrante du cycle de vie, plutôt que d'intervenir uniquement après le déploiement.

[8] OWASP, Top 10 for Large Language Model Applications
[9] OWASP, Top 10 for Agentic Applications for 2026



« La priorité pratique n'est pas d'éliminer le risque lié à l'IA, mais de le rendre gérable. Cela suppose d'attribuer des responsabilités claires, de fixer des limites à l'usage acceptable, de tester les processus intégrant l'IA et de préparer des plans de réponse pour les scénarios où les systèmes d'IA divulguent des données, fournissent des recommandations non fiables ou agissent au-delà de l'autorité qui leur a été conférée. »

Joani Green,
Global Technical Director,
Cyber Security at S-RM

Sécuriser l'IA dès sa conception

Les organisations qui intègrent dès le départ la sécurité à leurs projets d'IA seront mieux préparées à déployer cette technologie à grande échelle et à renforcer leur résilience à long terme, au fil de l'évolution de la réglementation. La technologie ne suffit pas, à elle seule, à atteindre cet objectif.

Les cinq priorités suivantes constituent un socle opérationnel pour repérer rapidement les risques et adopter l'IA en toute confiance :

Une meilleure gouvernance des données

Une gouvernance robuste de l'IA commence par la compréhension des données qui alimentent les systèmes. Les organisations doivent savoir à quelles informations leurs systèmes d'IA ont accès, d'où elles proviennent et comment elles sont protégées, afin de réduire à la fois les risques réglementaires et les risques de sécurité.

Sécuriser les modèles et les applications

Les modèles d'IA doivent être traités comme des actifs critiques de l'entreprise. Les tests de sécurité, la surveillance continue et une gestion efficace du changement contribuent à maintenir la confiance dans les services intégrant l'IA et réduisent le risque de manipulation ou d'accès non autorisé.

Renforcer la gestion des identités et des accès

À mesure que les systèmes gagnent en autonomie, la gestion des identités et des accès devient plus importante. Cette approche est conforme aux recommandations des Top 10 OWASP pour les applications LLM [8] et pour les applications agentiques [9], qui placent l'autonomie excessive des agents et les autorisations trop étendues parmi les risques de sécurité émergents les plus importants. Les organisations doivent veiller à ce que les utilisateurs comme les systèmes d'IA n'accèdent qu'aux données et aux applications nécessaires à leur rôle. Cette approche renforce la gouvernance tout en limitant les conséquences de la compromission d'un compte.

Renforcer la résilience de l'ensemble de l'écosystème de l'IA

La plupart des organisations s'appuient sur un réseau de fournisseurs de services cloud, de partenaires technologiques et de prestataires d'IA. Comprendre ces interdépendances aide à gérer cet écosystème et à identifier d'éventuelles faiblesses à un stade précoce.

Surveiller en continu et s'adapter

L'IA n'est pas statique : les modèles évoluent constamment, la réglementation change et de nouvelles menaces émergent. La surveillance continue, les revues de gouvernance et les tests peuvent aider les entreprises à détecter les problèmes rapidement, à démontrer le maintien de la conformité et à s'adapter à l'évolution des technologies et des risques.

En définitive, la sécurité dès la conception vise à donner aux organisations la confiance nécessaire pour innover et déployer l'IA de manière sûre et responsable, en intégrant la confiance à chaque étape du processus. Cela implique d'intégrer la gouvernance, la sécurité et la résilience à chaque étape de l'adoption, avec le soutien d'une culture organisationnelle adaptée et, si nécessaire, de partenaires de confiance capables d'aider les organisations à évoluer dans un paysage de risques de plus en plus complexe.

[8] OWASP, Top 10 for Large Language Model Applications

[9] OWASP, Top 10 for Agentic Applications for 2026

L'approche AXA XL

La résilience repose d'abord sur une vision claire des usages. Les organisations doivent savoir où l'IA est utilisée, à quelles données elle peut accéder, quelles décisions elle influence et de quels tiers elle dépend. Cela inclut les initiatives formelles d'IA ainsi que les usages plus discrets au moyen d'outils publics, de fonctionnalités logicielles intégrées et d'agents d'IA autonomes.

AXA XL considère que la gestion des risques liés à l'IA doit être fondée sur des scénarios métier concrets. Les organisations doivent envisager ce qui se passerait si un modèle produisait des résultats non fiables, si un agent d'IA agissait au-delà de son autorité, si des données sensibles étaient divulguées au moyen d'un prompt ou si un fournisseur critique d'IA devenait indisponible.

Ces scénarios permettent de traduire des vulnérabilités techniques en conséquences concrètes pour l'entreprise, telles que des pertes financières, des perturbations opérationnelles, une mise en cause de la responsabilité, une surveillance réglementaire accrue et une atteinte à la réputation. Ils facilitent également des échanges plus clairs sur la résilience et l'assurance.

Les pertes liées à l'IA peuvent ne pas correspondre à une catégorie unique de risques. Une fraude au paiement rendue possible par un hypertrucage (« deepfake »), une fuite de données liée à l'IA, une réponse défectueuse causant une perte à un tiers ou une panne chez un fournisseur critique peuvent mobiliser différentes composantes du programme de gestion des risques et d'assurance de l'organisation.

Comprendre ces scénarios en amont aide à déterminer dans quels cas les contrôles et les garanties existants peuvent s'appliquer, où subsistent des incertitudes et où des mesures d'atténuation supplémentaires peuvent être nécessaires.

AXA XL associe le conseil en gestion des risques, l'expertise cyber et le savoir-faire en assurance pour soutenir cette vision élargie de la résilience liée à l'IA. En collaboration avec des partenaires spécialisés tels que S RM, AXA XL aide les organisations à identifier leur exposition, à renforcer leur gouvernance, à se préparer aux scénarios d'incidents émergents et à prendre des décisions plus éclairées sur le transfert des risques.

L'objectif n'est pas de freiner l'innovation, mais de permettre aux organisations d'adopter l'IA en toute confiance : comprendre où se situent les risques, les gérer grâce à une gouvernance et à une résilience renforcées, puis évaluer dans quelle mesure ils peuvent être transférés ou assurés.

À mesure que l'IA s'intègre aux principaux processus métier, les organisations doivent comprendre comment elle modifie leur profil de risque global. L'IA ne doit pas être considérée uniquement comme un risque technologique, mais comme un enjeu de résilience pour l'entreprise, qui englobe la cybersécurité, la gouvernance des données, les dépendances aux tiers, la continuité opérationnelle, la responsabilité réglementaire et l'assurance.

Perspectives

L’adoption de l’IA ne montre aucun signe de ralentissement. Le principal défi pour les entreprises consiste donc à veiller à ce que cette technologie puisse être déployée de manière fiable à grande échelle.

Cela suppose de comprendre comment l’entreprise utilise l’IA, d’intégrer la gouvernance dans l’ensemble de son cycle de vie et de veiller à ce que la sécurité évolue au même rythme que la technologie. Les organisations qui posent ces fondations dès aujourd’hui seront mieux préparées à s’adapter à l’évolution des menaces et de la réglementation.

Construire une IA de confiance exige également une collaboration étroite entre les équipes dirigeantes et les fonctions de gestion des risques, juridiques, de sécurité et opérationnelles, avec le soutien de partenaires qui comprennent à la fois les opportunités offertes par l’IA et les défis qu’elle présente.

Les organisations qui intégreront la gouvernance, la sécurité et la résilience dans leur mode de fonctionnement seront celles qui exploiteront pleinement le potentiel de l’IA et s’adapteront en toute confiance, à mesure que cette technologie puissante continue d’évoluer.

Avertissement

Ce rapport est le résultat d'analyses provenant d'une grande variété de sources, parmi lesquelles des rapports publics, des analyses et des insights, ainsi que des analyses et insights propriétaires d'AXA XL et de S RM fondés sur leurs données internes. Une liste non exhaustive de sources publiques est incluse dans le rapport, mais ne constitue pas l'unique source des éléments ayant permis ce travail.

Les analyses présentées dans ce rapport reposent sur les informations disponibles au moment de la rédaction. Lorsque des évolutions futures sont évoquées, il ne s'agit pas de prédictions quant à l'évolution des tendances et des menaces, mais de la description du contexte possible dans lequel les organisations pourraient devoir opérer.

Global Asset Protection Services, LLC, XL Catlin Services SE et leurs affiliés (« AXA XL Risk Consulting ») fournissent des rapports de prévention des pertes et d'évaluation des risques ainsi que d'autres services de risk consulting, sur demande. À cet égard, nos publications, services et visites de prévention des pertes en matière de biens ne traitent pas des questions de sécurité des personnes ou de responsabilité envers des tiers.

Ce document ne doit pas être interprété comme une indication de l'existence ou de la disponibilité, dans le cadre de quelque police d'assurance que ce soit, d'une couverture pour un type particulier de perte ou de dommage. La fourniture de tout service n'implique pas que tous les dangers possibles aient été identifiés sur un site ni qu'aucun autre danger n'existe. AXA XL Risk Consulting n'assume, et n'aura, aucune responsabilité pour le contrôle, la correction, la poursuite ou la modification de conditions ou d'opérations existantes.

Nous déclinons spécifiquement toute garantie ou représentation selon laquelle le respect de tout conseil ou recommandation formulé dans ce document ou dans toute autre communication rendrait un site ou une opération sûr ou sain, ou les placerait en conformité avec une norme, un code, une loi, une règle ou une réglementation quelconque.

Sauf accord exprès écrit, AXA XL Risk Consulting et ses sociétés liées et affiliées déclinent toute responsabilité pour les pertes ou dommages subis par toute partie découlant de ou liés à nos services, y compris les pertes ou dommages indirects ou consécutifs, quelle qu'en soit l'origine. Toute partie choisissant de s'appuyer de quelque manière que ce soit sur le contenu de ce document le fait à ses propres risques.

Les informations contenues dans ce document sont fournies à titre purement informatif. La couverture d'assurance dans un cas particulier dépendra du type de police en vigueur, des termes, conditions et exclusions de ladite police, ainsi que des faits propres à chaque situation.

Aucune déclaration n'est faite quant à l'applicabilité de quelque couverture d'assurance spécifique que ce soit dans les circonstances décrites ici. Veuillez vous référer aux formulaires de police individuels pour connaître les détails spécifiques des couvertures. Ce résumé ne constitue ni une offre, ni une sollicitation ni une publicité dans quelque juridiction que ce soit, ni ne se veut une description de produits ou services d'AXA XL.

AXA XL est une division du Groupe AXA fournissant des produits et services via trois groupes d'activité : AXA XL Insurance, AXA XL Reinsurance et AXA XL Risk Consulting.

Aux États Unis, les compagnies d'assurance AXA XL sont : AXA XL Insurance Company Americas, Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Specialty Insurance Company et AXA XL Excess & Surplus Lines Insurance Company.

Au Canada, les garanties d'assurance sont souscrites par XL Specialty Insurance Company – succursale canadienne.

Aux Bermudes, la compagnie d'assurance est XL Bermuda Ltd. Certaines couvertures peuvent également être souscrites par le Lloyd's Syndicate n°2003.

Les couvertures souscrites par le Lloyd's Syndicate n°2003 sont placées au nom du membre du Syndicate n°2003 par Catlin Canada Inc. Les notations du Lloyd's sont indépendantes de celles du Groupe AXA.

Toutes les compagnies d'assurance ne sont pas actives dans toutes les juridictions et les garanties ne sont pas disponibles dans toutes les juridictions.

axaxl.com/fr