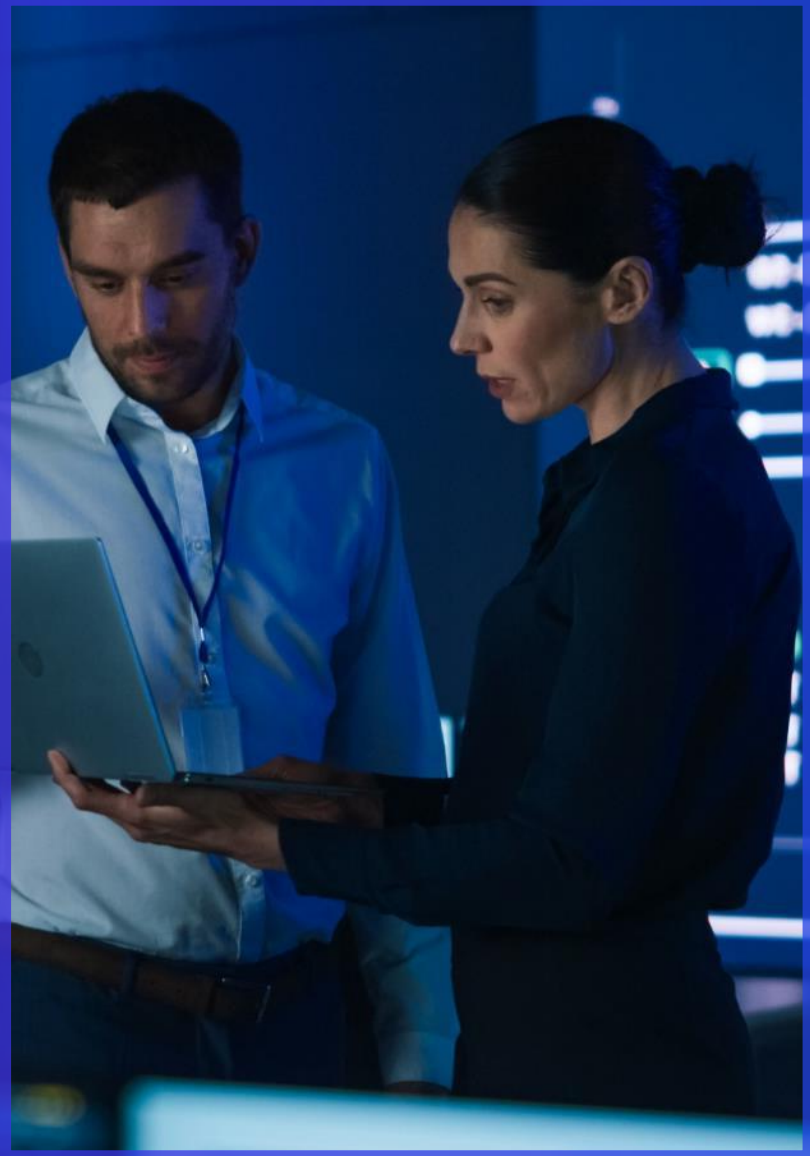
KPMG

Gestion des principaux risques liés aux opérations impliquant des systèmes d'IA exclusifs



Atténuer les risques pour maximiser la valeur des transactions

Janvier 2023

Introduction

01 **Nous constatons un recours croissant aux technologies d'intelligence artificielle (IA) dans des processus opérationnels clés dans tous les secteurs d'activité, et une intensification de l'activité transactionnelle dans le domaine de l'IA.**

02 **Cependant, les fusions et acquisitions impliquant de telles technologies peuvent entraîner plusieurs risques liés à la sécurité des données ainsi que des risques commerciaux, technologiques et organisationnels.**

03 **Nous vous présentons un cadre contenant les éléments clés que doivent prendre en considération les acheteurs pour atténuer ces risques.**

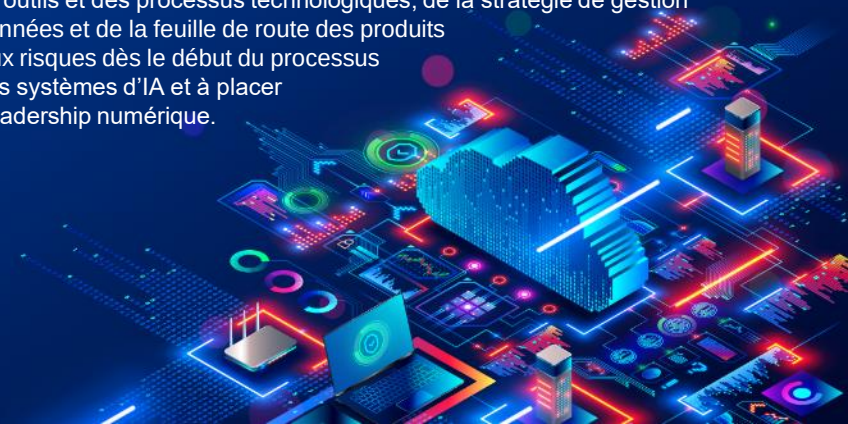
Le présent livre blanc s'inscrit dans une série d'études illustrant l'importance du rôle des TI pour accroître la valeur des transactions et réduire les risques d'entreprise en cours d'opération. Cette série met également en lumière les principes que l'équipe Fusions et acquisitions en TI de KPMG au Canada exploite pour atténuer les risques et maximiser la valeur pour leurs clients de divers secteurs.

Dans le marché d'aujourd'hui, on observe une tendance croissante de l'intelligence artificielle; une intelligence démontrée par les machines qui aide les entreprises modernes à accroître leurs revenus et leurs économies sur les coûts d'exploitation. En particulier, l'applicabilité des technologies d'IA dans diverses situations a permis a des organisations de multiples secteurs – dont les services informatiques, les soins de santé, la cybersécurité, les services financiers, le commerce de détail, la fabrication, le transport et la logistique – de créer de la valeur.

Compte tenu des avantages de l'IA, les entreprises et les sociétés de capital-investissement acquièrent progressivement des sociétés qui exploitent ses capacités. Selon le rapport mondial sur le marché de l'IA publié par Drake Star Partners, les fusions et acquisitions dans le domaine de l'IA ont sextuplé depuis 2015, les transactions déclarées en 2021 atteignant la valeur totale de 12,3 milliards de dollars. Bien que les services informatiques mènent sur le plan du volume de capital investi, le secteur de la cybersécurité a connu la plus forte augmentation du nombre de transactions, avec un stupéfiant taux de croissance annuel composé de 135 % entre 2016 et 2021. De plus, les observations canadiennes tirées d'un sondage mondial mené par KPMG International révèlent que 95 % des dirigeants en technologie dans les organisations des secteurs privé et public au Canada prévoient investir dans le Web3. En outre, 70 % comptent investir dans la 5G et l'informatique en périphérie, 67 % entendent tirer parti de l'informatique quantique et 54 % prévoient investir dans le métavers au cours de la même période. Toutes ces technologies reposent sur l'IA pour alimenter leurs cas d'utilisation respectifs.

Alors que l'IA s'intègre de plus en plus aux processus organisationnels, nous avons constaté qu'un certain nombre de risques liés à la sécurité des données ainsi que de risques commerciaux, technologiques et organisationnels entravent la création de valeur dans le contexte des transactions. L'objectif de ce livre blanc est de présenter un cadre qui permet aux acheteurs d'identifier et d'atténuer de façon proactive ces risques au cours de la phase de contrôle diligent préalable à la transaction afin de créer de la valeur à partir de systèmes d'IA exclusifs après celle-ci.

Ce cadre peut aider à structurer l'évaluation des outils et des processus technologiques, de la stratégie de gestion des talents, des mécanismes de sécurité des données et de la feuille de route des produits du vendeur. Une gestion proactive des principaux risques dès le début du processus d'acquisition peut aider à maximiser la valeur des systèmes d'IA et à placer l'acheteur sur la voie du succès en matière de leadership numérique.



Principaux risques liés à l'acquisition

Bien que l'utilisation de l'IA par les dirigeants du domaine numérique puisse donner lieu à des avantages commerciaux tangibles, les acheteurs doivent tenir compte des risques suivants dans l'acquisition d'entreprises d'IA :

01. Risques commerciaux

Les vendeurs font souvent valoir la valeur commerciale qu'offrent les systèmes d'IA exclusifs, qui nécessitent habituellement plusieurs années de développement. Toutefois, ces systèmes pourraient être rapidement dépassés par les technologies d'IA prêtes à l'emploi, en particulier celles élaborées par des fabricants de logiciels agiles aux cycles de développement de produits rapides. Dans ces cas, le potentiel de revenus et la qualité commerciale des technologies acquises seraient limités.

02. Risques technologiques

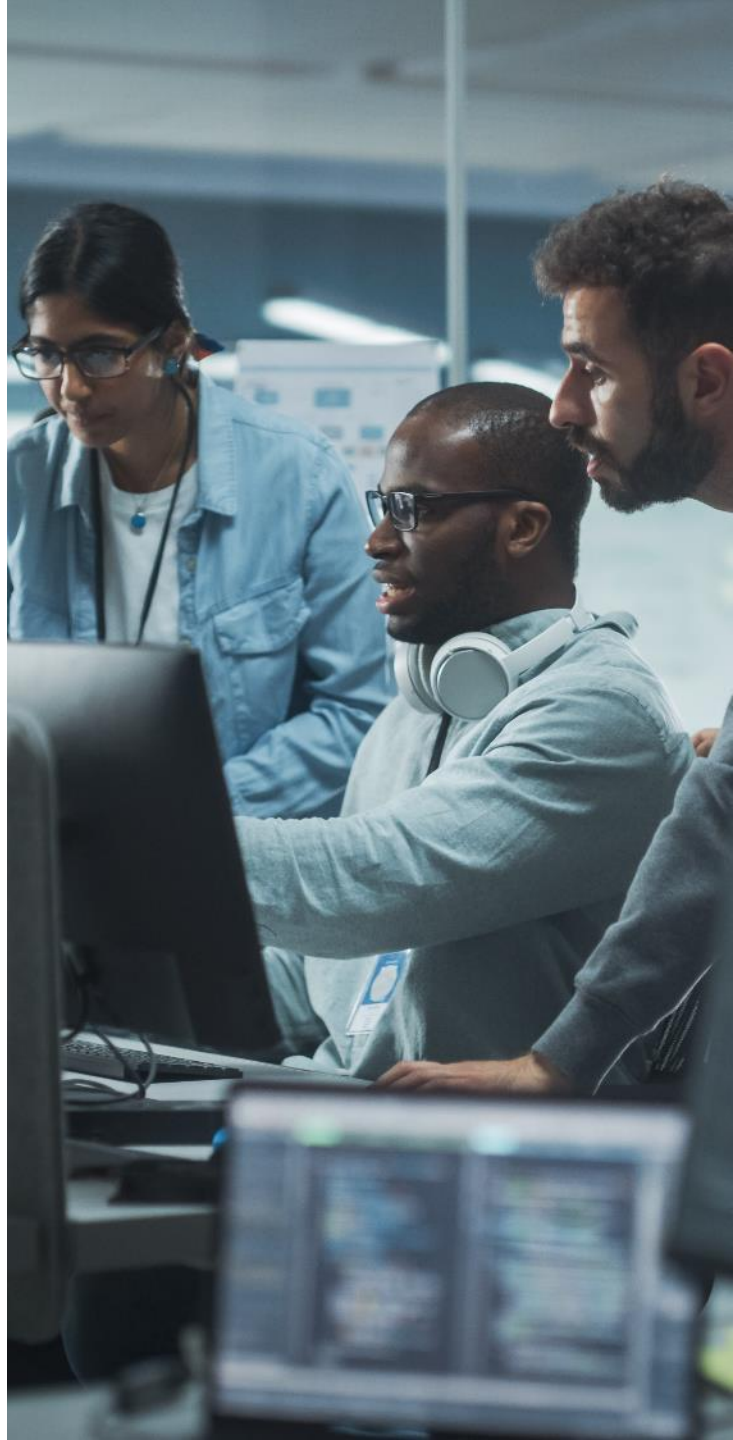
L'intégration des systèmes d'IA à l'environnement technologique après une acquisition nécessite la mise en place de plateformes de gestion des données complètes, le recours à des méthodes modernes de développement de logiciels et le renforcement des mécanismes permettant d'extraire des renseignements de l'analytique avancée. Cela exige des capacités technologiques solides, compétence que les acheteurs n'ont peut-être pas pleinement développée au moment de la transaction.

03. Risques organisationnels

Le rythme rapide de l'innovation en IA exige que le bassin de talents soit doté des compétences technologiques et opérationnelles requises et qu'il soit en mesure d'accroître rapidement les capacités de l'organisation pour répondre aux besoins opérationnels changeants. L'incapacité de trouver, d'embaucher et de fidéliser des talents appropriés peut constituer un risque en ce qui concerne la stratégie de l'acheteur visant à tirer pleinement parti de l'IA.

04. Risques liés à la sécurité des données

Les moteurs d'IA sont alimentés par les données, la plupart pouvant représenter des renseignements confidentiels sur les consommateurs ou de l'information exclusive. Le défaut de protéger ces données contre les cyberattaques peut engendrer des obligations juridiques pour l'acheteur, surtout dans les régions où les règles en matière de protection des données et de vie privée sont strictes, comme en Californie avec la *Loi sur la protection de la vie privée des consommateurs*.



Domaines à privilégier dans le contrôle diligent

Il est possible d'atténuer les principaux risques en appliquant le cadre suivant à la phase de contrôle diligent préalable à la transaction :

Domaines à privilégier dans le contrôle diligent

Feuille de route du produit réfléchie

Comparer la proposition de valeur de ce produit à celle des autres

Outils et processus technologiques solides

Vérifier que la maintenance du produit et des mises à jour futures sont possibles

Stratégie efficace de gestion des talents

Évaluer la qualité du bassin de talents en AI du vendeur pour maintenir et développer le produit

Mécanismes de sécurité des données fiables

Confirmer la résilience des cadres de sécurité contre les atteintes à la protection des données

Feuille de route du produit réfléchie : Dans le cadre de l'acquisition d'entreprises d'IA, il est important de confirmer que la technologie du vendeur est unique et qu'elle ne peut pas être reconstruite à l'aide d'outils et de solutions d'IA déjà disponibles sur le marché. De plus, la stratégie du produit doit être prise en compte dans le processus de contrôle diligent étant donné qu'elle dicte le degré de personnalisation des modules d'IA et leur applicabilité aux exigences commerciales de l'acheteur. Ces considérations sont importantes pour atténuer les **risques commerciaux**.

Outils et processus technologiques solides : L'acheteur doit vérifier que les outils et les processus technologiques du vendeur permettent la maintenance et la mise à jour périodique des technologies d'IA. Pour cela, il faut notamment que des trousses de développement d'IA et des modules de maintenance de fournisseurs réputés existent. Ces mesures proactives favorisent l'intégration harmonieuse des systèmes d'IA dans l'environnement technologique de l'acheteur, atténuant ainsi les **risques technologiques**.

Stratégie efficace de gestion des talents : À notre avis, même si la montée de l'IA semble éliminer l'utilité de l'élément humain, c'est plutôt le contraire qui est vrai. Des talents qualifiés sont encore nécessaires pour développer, surveiller et exploiter pleinement les plateformes d'IA. S'assurer que la stratégie du vendeur en matière de gestion des talents favorise ces compétences à l'interne et amène les bonnes personnes dans l'équipe est une étape importante dans l'atténuation **des risques organisationnels**.

Mécanismes de sécurité des données fiables : Une plateforme d'IA est principalement alimentée par les données qui génèrent ses algorithmes. Dans bien des cas, toutefois, les données détenues et gérées par le vendeur sont jugées confidentielles et sont soumises à des contraintes réglementaires. Le vendeur devrait donc se parer aux atteintes à la protection des données en mettant en place de solides contrôles et politiques de cybersécurité visant à atténuer les **risques liés à la sécurité des données**.

Un examen attentif des risques susmentionnés et l'exécution méthodique des mesures d'atténuation favoriseront la création de valeur pour les acheteurs après la transaction.

Étude de cas

Voici un exemple concret de contrôle diligent préalable à l'acquisition d'une société de soins de santé ayant élaboré un système d'IA exclusif. Le système, hébergé sur place, est doté de plusieurs fonctionnalités, dont la modélisation prédictive fondée sur l'IA pour la détection précoce des maladies à l'aide de données tirées de dossiers de santé électroniques et l'automatisation intelligente pour la vérification de la facturation. Le contrôle diligent visait principalement à identifier les risques liés au système d'IA pour l'investisseur privé, lequel prévoyait d'élargir l'étendue des activités de l'entité acquise aux États-Unis et au Canada après la transaction. Bien que le vendeur ait offert une proposition de valeur unique permettant une viabilité commerciale et qu'il ait élaboré une feuille de route du produit qui tenait compte des exigences relatives à la personnalisation future, des risques potentiels pour l'acheteur demeuraient :

Risque technologique : Utilisation d'anciens outils de développement dotés d'une capacité de maintenance et de mise à niveau limitées.

Risque organisationnel : Dépendance des personnes clés aux employés qui ont participé à la conception et à l'élaboration du système exclusif.

Risque lié à la sécurité des données : Non-conformité à la *Health Insurance Portability and Accountability Act* (HIPAA), une réglementation des États-Unis qui prévoit des dispositions pour protéger les données sur les patients.

Afin d'atténuer ces risques, nous avons recommandé les mesures suivantes en tenant compte de l'envergure des activités actuelles et futures, des contraintes de temps associées à la transaction et des incidences sur le plan des coûts :

Passer à la suite de produits d'IA offerts sur la plateforme **Microsoft Azure**. Celle-ci fournit des outils et des processus pour concevoir, lancer et mettre en œuvre le système d'IA ainsi qu'une maintenance et des mises à jour automatiques de la plateforme de développement. Cela permet d'atténuer le **risque technologique** et de minimiser les coûts de maintenance continue du système d'IA.

Tirer parti de la solution **Azure DevOps de Microsoft**. La création d'un répertoire complet de tous les logiciels et artefacts liés à l'IA permet de conserver les connaissances exclusives en cas de départs d'employés clés, et par le fait même, d'atténuer le **risque organisationnel** et de réduire au minimum les coûts de main-d'œuvre associés à la reconstruction éventuelle de la base de connaissances en IA.

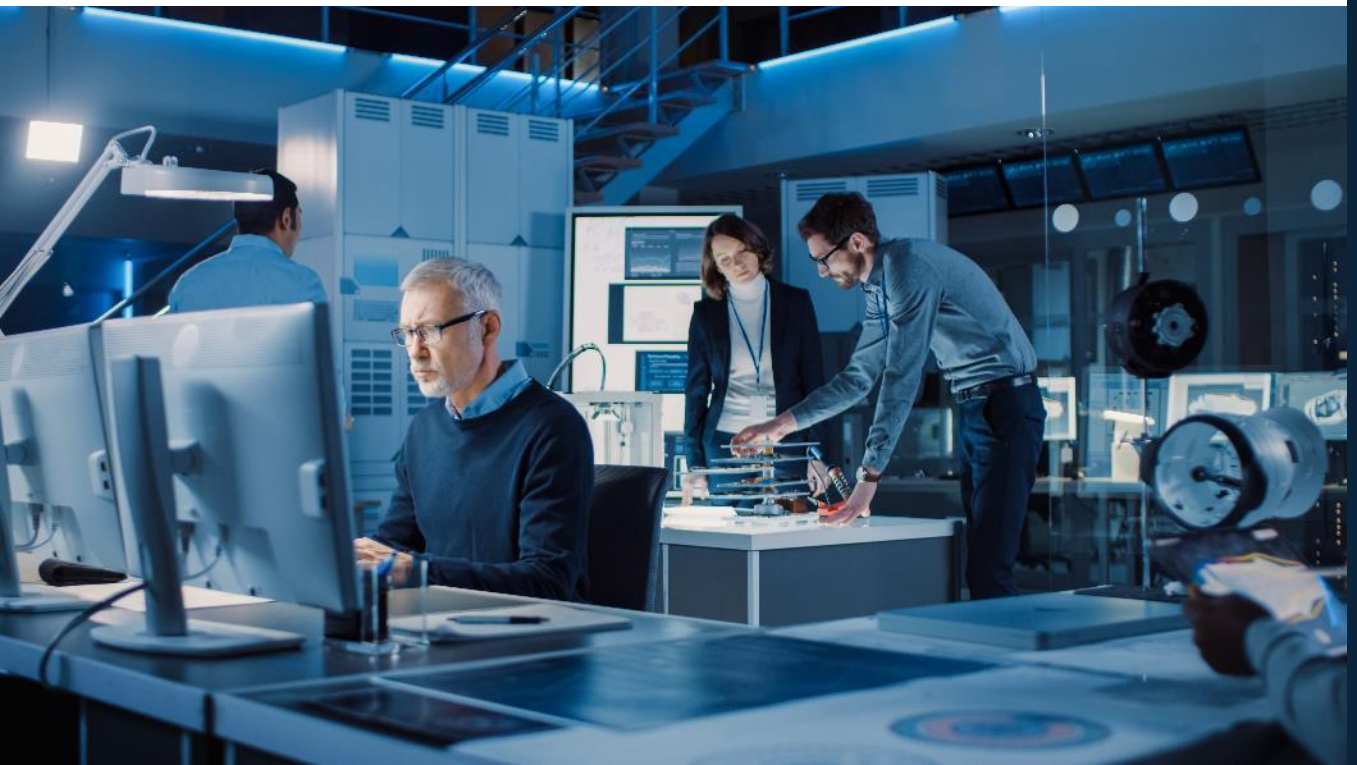
Adopter le **cadre de cybersécurité du National Institute of Science and Technology**. Celui-ci englobe les normes de sécurité relatives aux données sur les patients afin d'assurer l'harmonisation avec les exigences réglementaires de la HIPAA. De plus, il présente la plateforme de protection de la propriété intellectuelle du module **Azure Machine Learning de Microsoft**, qui sécurise les ensembles de données exclusives utilisés pour former le modèle d'IA afin d'atténuer le **risque lié à la sécurité des données** et de réduire les frais juridiques découlant de cyberattaques potentielles ciblant les données sur les patients.

L'exécution tactique des mesures susmentionnées a atténué les risques liés à la transaction tout en réduisant les frais juridiques ainsi que les coûts de maintenance et de main-d'œuvre. Par conséquent, les mesures prises avant la transaction ont ajouté de la valeur à l'investissement de l'acheteur et permettent de tirer parti des avantages opérationnels du système d'IA après l'acquisition.

Résumé et conclusion

Il est important que les acheteurs reconnaissent les risques liés à la sécurité des données ainsi que les risques commerciaux, technologiques et organisationnels associés à l'acquisition de sociétés qui possèdent des systèmes d'IA exclusifs. Une évaluation préliminaire durant la phase de contrôle diligent préalable à la transaction peut aider à identifier et à atténuer ces risques potentiellement significatifs, en plus d'aider l'acheteur à maximiser la valeur en favorisant la production de recettes et en augmentant les économies sur les coûts d'exploitation.

Pour savoir comment KPMG peut vous aider à relever les défis liés à l'IA et à tirer le plein potentiel de votre fusion ou acquisition, n'hésitez pas à communiquer avec nous.



Communiquez avec l'équipe Fusions et acquisitions en TI

Sharjil Salim
Associé
Toronto, Canada
416-791-2030
ssalim1@kpmg.ca

Aditya Narasimha
Directeur
Toronto, Canada
416-791-2104
anarasimha@kpmg.ca