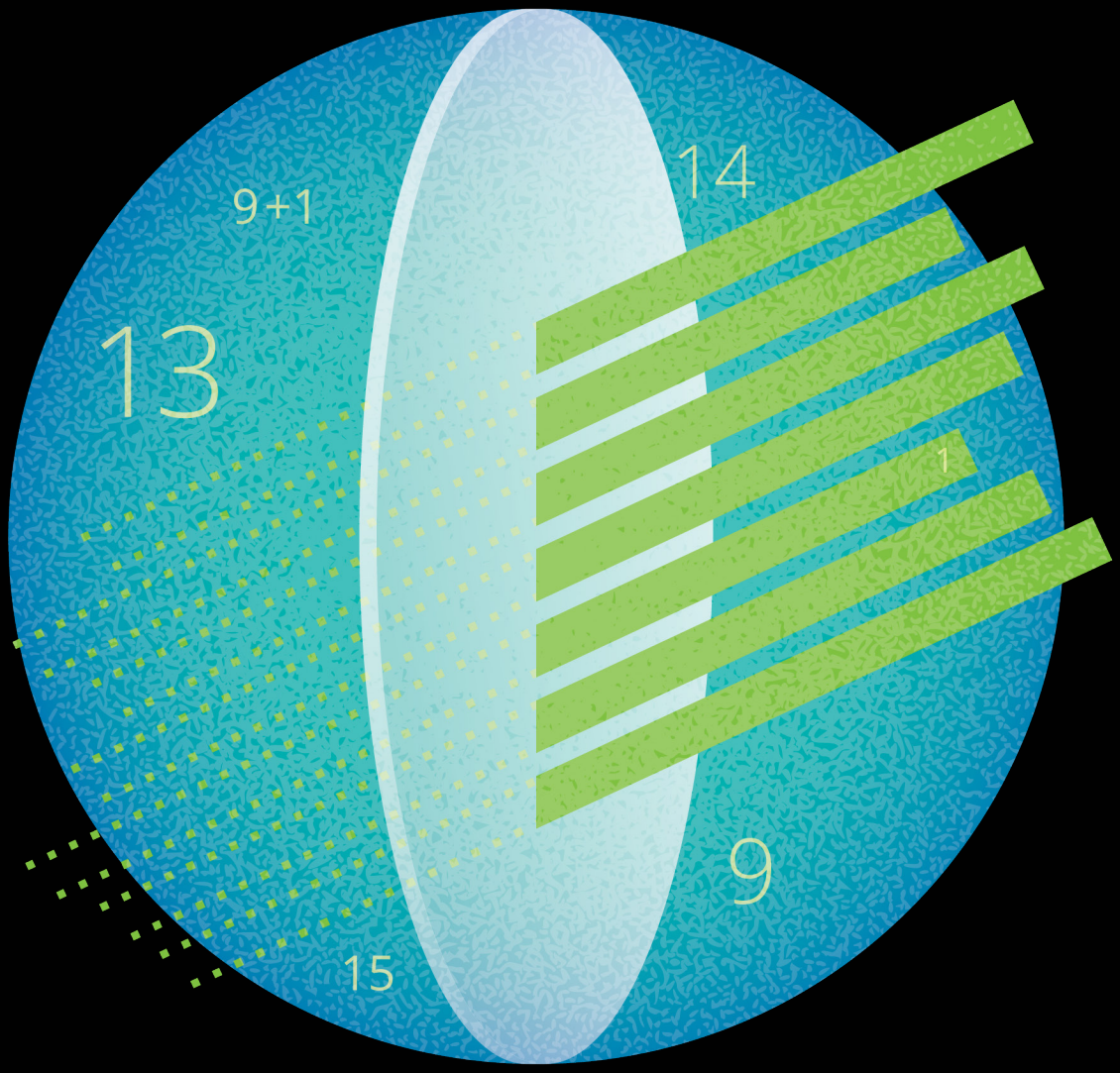
Deloitte.



Omnia IA

Bâtir la confiance envers l’IA

Comment surmonter les risques et opérationnaliser la gouvernance de l’IA

Table des matières

Introduction

L'intelligence artificielle (IA) est considérée comme l'un des principaux catalyseurs de l'innovation dans presque tous les secteurs. Les organisations ont néanmoins tardé à l'adopter en raison des difficultés et des aspects inconnus qu'elle présente. La démystification des risques inhérents à l'IA est une étape clé pour surmonter ces difficultés et mieux comprendre comment extraire la valeur de l'IA.

Même si le contexte réglementaire continue d'évoluer, les organisations peuvent commencer à s'attaquer aux risques liés à l'IA, une démarche qui nécessite une gouvernance robuste, transparente et axée sur la technologie. La mise en place de l'IA de confiance n'est pas un processus isolé; elle est le fruit de l'effort collectif de toute l'entreprise. Pour y parvenir, les organisations doivent tenir compte de trois questions clés : À quel moment doit-on mettre en œuvre des mécanismes de gouvernance? Qui en assume la responsabilité? Comment opérationnaliser la gouvernance et habiliter l'organisation?

En collaborant directement avec les organisations clientes pour accélérer leur adoption de l'IA, Deloitte a créé le cadre de l'IA de confiance afin de décrire les capacités nécessaires à une gouvernance efficace. Poursuivez votre lecture afin d'en savoir plus.

Exploiter les occasions liées à l'IA

Des améliorations au fil du temps à la réinvention totale, les acteurs établis et les nouveaux venus dans un éventail de secteurs cherchent à exploiter le potentiel de l'IA pour réduire les coûts et accélérer l'innovation.

Lorsqu'elle est correctement appliquée, l'IA peut avoir une incidence importante sur les facettes suivantes des activités d'une organisation :

MODELER DES OPÉRATIONS ALLÉGÉES ET PLUS RAPIDES
L'IA peut contribuer à améliorer l'efficacité et à réduire les coûts

FOURNIR DES PRODUITS ET DES CONSEILS ADAPTÉS
L'IA peut faciliter la personnalisation des services tout en assurant l'adaptabilité

ÊTRE OMNIPRÉSENT
L'IA peut contribuer à mettre des produits et services à la portée des clients au moment, à l'endroit et de la manière dont ils ont en besoin

FAVORISER LA PRISE DE DÉCISIONS PLUS INTELLIGENTE
L'IA permet de traiter de grands volumes de données afin de dégager de meilleures perspectives d'affaires

DÉCOUVRIR DE NOUVELLES PROPOSITIONS DE VALEUR
L'IA peut contribuer à l'élaboration de nouvelles offres et de nouvelles façons de travailler

Malgré les occasions exceptionnelles que présente l'IA, de nombreuses organisations ont mis plus de temps que prévu à libérer son potentiel. Nous avons exploré les raisons de cette adoption tardive dans notre rapport intitulé *Impératif de l'IA au Canada*, mais sachez que la confiance est un facteur de taille. Les contextes réglementaires incertains, la sécurité et la confidentialité des données, et l'atteinte à la réputation présentent tous des risques.

Heureusement, il existe une approche qui permet aux organisations de faire progresser leurs démarches en IA en toute confiance. La première étape consiste à tenir compte des risques.

Tenir compte des risques

Parce que l'IA est une nouvelle technologie peu connue, et que les erreurs peuvent avoir des conséquences importantes, les organisations sont réticentes à l'adopter. Pour gérer les risques stratégiques, financiers et d'atteinte à la réputation connexes, il importe d'abord de comprendre les risques inhérents à la conception, au développement, au déploiement et à l'entretien des systèmes d'IA.

Comprendre les risques liés à l'IA

Risques d'affaires

Les risques d'affaires englobent les risques stratégiques, financiers et d'atteinte à la réputation auxquels une organisation peut s'exposer en utilisant ou en développant des technologies d'IA.

Sources de risque

Les organisations devront gérer quatre sources prédominantes de risques liés à l'IA :

Données

… y compris les renseignements concernant la collecte, l'utilisation et la transmission.

Modèles

… qui tirent des prédictions et des perspectives des données.

Technologies

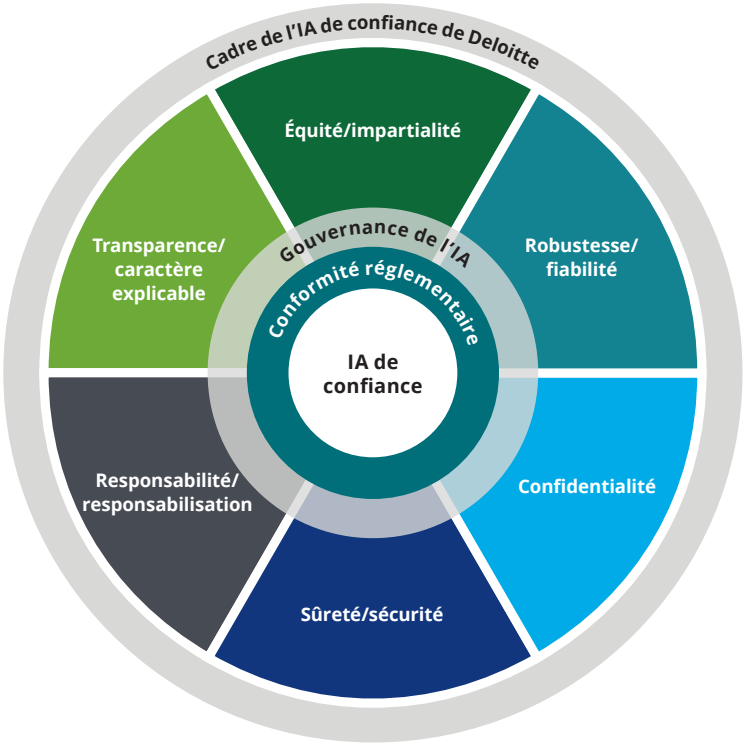
… et des processus qui forment l'ensemble du système d'IA.

Interaction

… entre les gens et les systèmes d'IA dans la prise de décisions et de mesures.

Ces sources peuvent amener les organisations à faire des progrès dans l'élaboration de stratégies et de politiques d'atténuation des risques. La sélection prudente des données, la détermination des façons dont elles peuvent être utilisées et les décisions de gouvernance qui sont prises au cours de la création du modèle d'IA sont des exemples des moyens dont les organisations disposent pour atténuer les risques et mettre en place des systèmes d'IA de confiance.

Cadre de l'IA de confiance de Deloitte



Conformité

Les organisations font face aux incertitudes attribuables au contexte réglementaire. Les règlements qui s'appliquent à l'IA varient selon le niveau de maturité, et selon le territoire et le secteur. Alors que les organismes de réglementation s'empressent de définir la portée, l'applicabilité et le caractère exécutoire des règlements, le contexte juridique avec lequel les organisations interagissent peut aussi évoluer rapidement. Aussi, les organisations devront suivre leur évolution et être prêtes à s'adapter rapidement pour respecter les nouvelles directives. On s'attend à ce que les règlements liés à l'IA couvrent largement les domaines de risques inhérents à l'IA.

Risques inhérents à l'IA

Le cadre de l'IA de confiance de Deloitte a six domaines de risques, indiqués ci-dessous, qui doivent être identifiés et atténués. En collaboration avec nos clients, nous avons trouvé deux domaines de risques complémentaires qui peuvent chevaucher les six domaines de risques principaux ou être traités de manière distincte.

Équité/impartialité	Robustesse/fiabilité
Il incombe aux organisations d'assurer que les systèmes d'IA ne créent ou ne perpétuent pas de partis pris, et que les groupes sont traités d'une manière que l'organisation considérerait comme équitable.	Les organisations doivent s'assurer que leurs systèmes d'IA produisent des résultats cohérents et fiables, et qu'ils effectuent les tâches (et échouent parfois) comme prévu.
Confidentialité	**Sûreté/sécurité**
Les organisations doivent s'assurer que leurs systèmes d'IA sont développés et déployés en fonction du consentement et des droits à la protection des renseignements personnels des personnes, et qu'ils sont en mesure de protéger efficacement les renseignements personnels.	Les organisations doivent s'assurer de tenir compte des risques externes, physiques et numériques, entre autres, et les communiquer aux utilisateurs.
Responsabilité/responsabilisation	**Transparence/caractère explicable**
Les organisations doivent exposer clairement les rôles et responsabilités continus des personnes, des groupes et des fonctions pour assurer la fiabilité d'un système d'IA.	Les organisations doivent comprendre, interpréter et, dans bien des cas, communiquer la façon dont les données sont utilisées, et dont les systèmes d'IA prennent des décisions.

Domaines de risques complémentaires

Utilisation acceptable	Responsabilité des tiers
Les organisations doivent constamment évaluer les conséquences intentionnelles et non intentionnelles de leurs systèmes d'IA et vérifier leur harmonisation aux valeurs organisationnelles et sociétales.	Les organisations qui comptent sur des tiers pour les données et le développement, le déploiement ou l'entretien des systèmes ont la responsabilité de faire en sorte que ces tiers respectent les mêmes normes d'IA de confiance qu'elles respectent elles-mêmes.

Mettre à jour les processus de gestion des risques

Pour répondre efficacement aux risques liés à l'IA, il faudra assurer l'évolution des mécanismes existants de gestion des risques et la création de nouveaux processus de gouvernance consacrés à la mise en place de technologies d'IA de confiance.

Les mécanismes et processus existants de gestion des risques portant sur les technologies, la protection des renseignements personnels, la cybersécurité, la conformité, etc. devraient être mis à jour pour refléter les nouveaux moyens par lesquels les systèmes d'IA peuvent entraîner des risques. Par exemple, on pourrait mettre à jour le cadre de gestion des risques d'un tiers pour refléter les rôles que pourrait éventuellement jouer le tiers au sein d'un système d'IA, notamment celui de fournisseur de données, de développeur de modèles, de responsable de modèles et de fournisseur d'infrastructure informatique.

Il faut créer de nouveaux processus de gestion pour tenir compte des risques que l'organisation n'a peut-être pas été appelée à gérer par le passé, tels que le caractère explicable et l'utilisation acceptable. Les organisations doivent acquérir de nouvelles capacités qui leur permettront de déterminer, d'atténuer et de gérer ces risques.

Adopter une approche de gouvernance de l'IA axée sur le cycle de vie

Bien que les organisations comprennent l'importance de répondre aux risques associés à l'IA en créant de nouvelles pratiques de gestion des risques et en mettant à jour les pratiques existantes, il est aussi essentiel de ne pas négliger l'importance de choisir le bon moment d'agir.

Principales questions à prendre en considération au moment de déterminer quand la gouvernance doit être mise en place :

À quel moment faut-il déterminer les risques inhérents à un système d'IA?

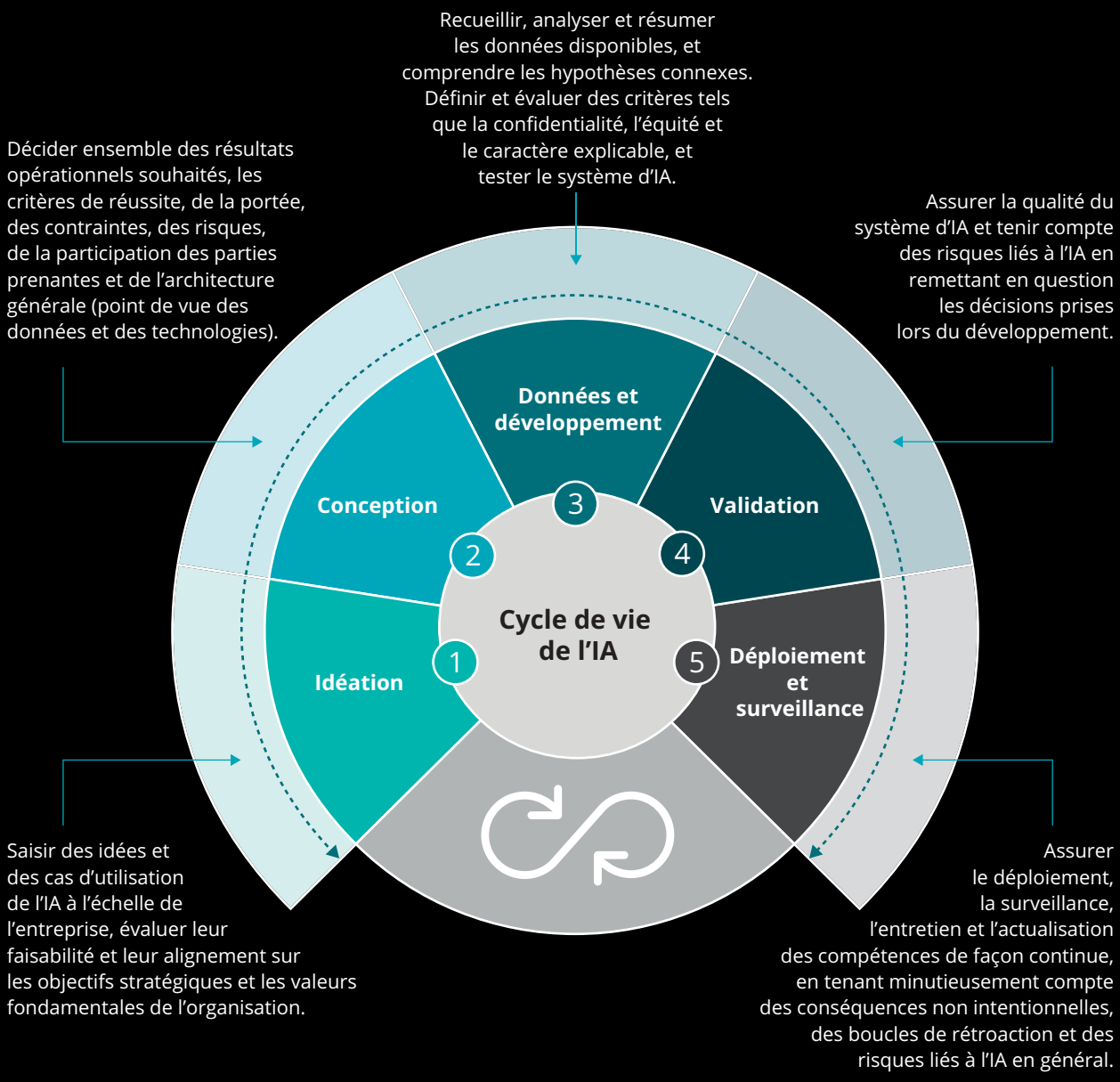
À quel moment faut-il répondre aux risques?

À quel moment faut-il déployer les activités de gouvernance de l'IA (p. ex., approbations, barrières, qualité, et contrôles)?

À quel moment les principales parties responsables et autres parties prenantes doivent-elles intervenir?

En répondant à ces questions au bon moment dans le cycle de vie de l'IA, les organisations seront en meilleure posture pour déterminer les risques et prendre des décisions éclairées à l'égard de la conception.

Le **cycle de vie de l'IA** aide les organisations à comprendre et à déterminer le meilleur moment pour mettre en place les mécanismes de gouvernance. Il représente les étapes distinctes et normalisées du développement d'un système d'IA. En voici un aperçu :



Le cycle de vie est illustré de façon linéaire, mais les organisations procéderont souvent à des itérations, particulièrement au cours des trois étapes intérieures. Plusieurs capacités de gouvernance de l'IA devraient être définies dans le contexte du cycle de vie de l'IA. D'autres ont une incidence plus générale sur l'organisation et ne sont pas associées à des systèmes d'IA individuels. Le cadre de l'IA de confiance de Deloitte met en évidence cette relation et précise les capacités nécessaires à une gouvernance robuste de l'IA.

Opérationnaliser la confiance envers l'IA

Stratégie d'entreprise → **Normes et règlements sectoriels** → **Normes et politiques internes**

Stratégies d'entreprise; normes et règlements sectoriels :
S'assurer que la stratégie d'entreprise de l'organisation intègre les priorités de développement et de déploiement de l'IA, et qu'elle tient compte des normes sectorielles et des règlements applicables.

Normes et politiques internes :
Veiller à ce que les risques additionnels liés à l'IA et les stratégies d'atténuation se reflètent dans les normes et politiques internes existantes (p. ex., confidentialité, sécurité, gestion des fournisseurs, etc.).

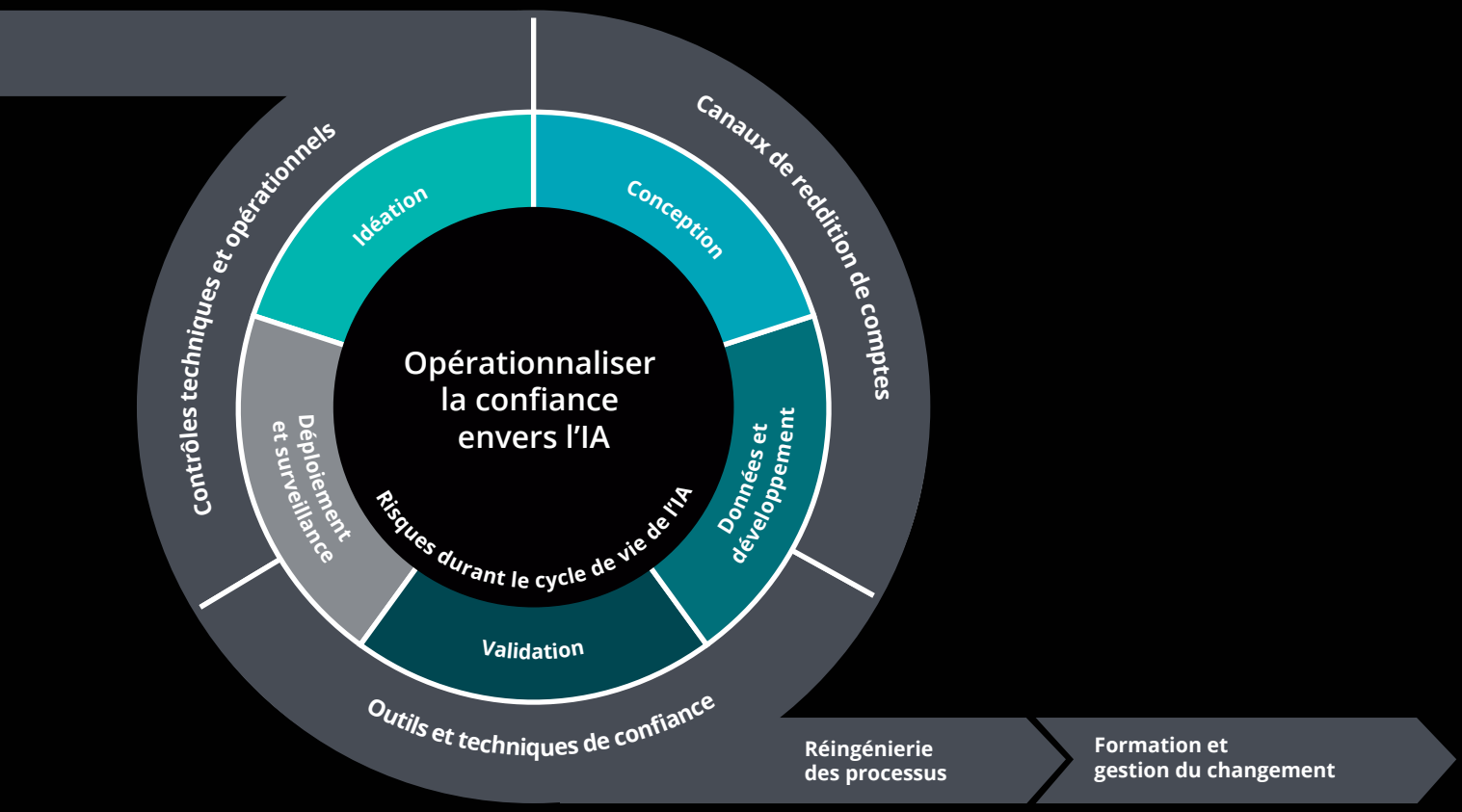
Contrôles :
Mettre en place des balises techniques dans le cadre de la conception des solutions d'IA afin d'éviter que certaines mesures précises soient prises.

Réingénierie des processus :
S'assurer que l'être humain fait partie du cycle aux étapes critiques où les risques liés à l'IA pour les consommateurs, les employés, les organismes de réglementation et le bénéfice net atteignent un niveau trop élevé.

Responsabilisation :
Tenir les équipes appropriées de l'organisation responsables des décisions concernant la sélection, le développement et le déploiement de cas d'utilisation et de systèmes d'IA, et les habiliter à remédier aux risques.

Outils et techniques :
Établir des outils permettant de surveiller les risques associés aux systèmes d'IA de façon dynamique. Intégrer des outils et techniques d'atténuation des risques et de renforcement de la confiance à la mise en place des applications d'IA en entreprise.

Formation et gestion du changement :
S'assurer que les clients, les employés, les actionnaires et les autres parties prenantes sont tenus au courant des points de vue, des perspectives et des mesures en ce qui a trait aux utilisations de l'IA.



Au-delà des capacités de gouvernance de l'IA de confiance mises en évidence, les organisations nécessiteront deux capacités fondamentales pour assurer une opérationnalisation efficace :

Gouvernance des données d'entreprise

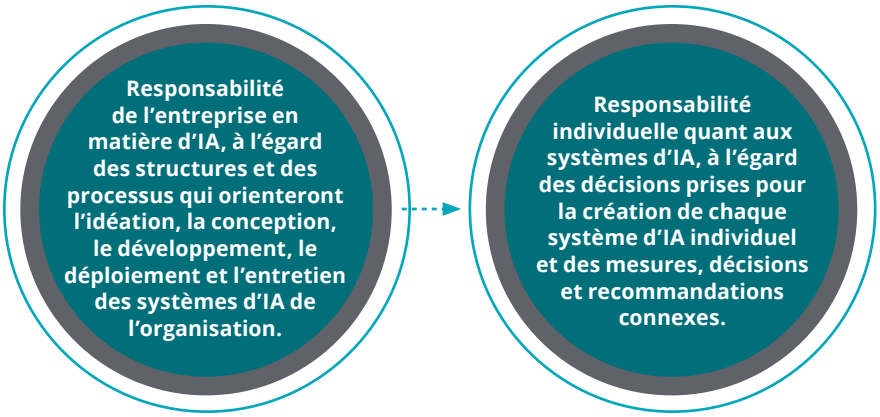
Des pratiques efficaces de gouvernance des données d'entreprise sont essentielles pour assurer que l'IA procure les avantages escomptés et qu'elle est arrimée à la stratégie d'entreprise. Quel que soit le niveau de maturité des capacités en matière de données, les organisations devraient investir dans un solide programme de gouvernance des données d'entreprise.

Gestion des risques d'entreprise

Les efforts consacrés à la gouvernance de l'IA et les pratiques de gestion des risques d'entreprise doivent être harmonisés et étroitement intégrés aux fins d'une opérationnalisation et d'une adoption efficaces. Les pratiques, principes et processus existants devraient être utilisés et améliorés afin de répondre aux risques associés à l'IA dans l'ensemble de l'entreprise.

Déterminer qui est responsable de la mise en place de l'IA de confiance

En travaillant avec nos clients, nous avons clairement établi le besoin de faire rapidement le point sur les responsabilités liées au parcours de gouvernance de l'entreprise en matière d'IA. Pour assurer la mise en œuvre de l'IA de confiance, la gouvernance d'entreprise doit reposer sur deux rapports de responsabilité :



Lorsqu'une organisation se dote d'une solide structure de reddition de comptes relativement à l'IA, la responsabilité individuelle quant aux systèmes d'IA est largement assurée. Il est possible de faire appel à un certain nombre de stratégies, telles que des forums, des équipes et des processus, pour assurer une responsabilisation rigoureuse de l'entreprise en matière d'IA. Nous avons observé quelques stratégies qui se sont avérées efficaces.

Comité de surveillance de l'IA

Les dirigeants et membres du conseil d'administration peuvent se demander s'ils disposent des forums appropriés pour prendre des décisions au sujet du développement et du déploiement de l'IA. Ils doivent aussi établir la présence de rapports de responsabilité des hauts dirigeants, et déterminer si les bonnes personnes sont représentées au sein de la gouvernance de l'IA. À cette fin, il est primordial de mettre en place un comité d'IA de confiance réunissant des représentants des gammes de services, des technologies, de la gestion des risques et d'autres groupes et fonctions critiques (p. ex., services juridiques, réglementation, confidentialité, déontologie), ainsi que des experts en IA. Son mandat devrait consister à faire respecter l'engagement de l'organisation à mettre en place l'IA de confiance, tout en établissant une gouvernance robuste de l'IA avant et pendant son utilisation concrète.

Centre d'excellence de l'IA

La plupart des organisations adoptent un modèle de centre d'excellence fédéré pour la mise en place des systèmes d'IA, où la conception et la dotation en personnel du centre sont axées sur le soutien de différents groupes ou fonctions, et où elles fournissent elles-mêmes l'expertise technique nécessaire pour accélérer l'adoption de l'IA dans ces domaines. Bon nombre d'entre elles ont confié au centre d'excellence en IA la tâche d'assurer la formation et la sensibilisation à l'IA à l'échelle de l'organisation. Cela dit, les organisations devraient aussi considérer que leur centre d'excellence en IA pourrait également s'acquitter des responsabilités suivantes :

- Habiliter, régir et orienter l'entreprise en ce qui a trait au développement et au déploiement responsables des systèmes d'IA, en prenant en charge certaines des activités de surveillance qui permettent d'instaurer la confiance envers l'IA;
- Favoriser le déploiement de solutions d'IA responsables, ce qui comprend la création, l'acquisition et la gestion des outils dont l'organisation a besoin pour mettre en place des systèmes d'IA de confiance;
- Diffuser des rapports et des perspectives à l'échelle de l'entreprise (p. ex., sur l'adoption de l'IA, l'inventaire d'IA).

Examen critique indépendant

Certaines organisations, notamment dans le secteur des services financiers, possèdent des équipes de validation de modèles bien établies et des cadres de gestion des risques liés aux modèles alignés sur les directives réglementaires de leur secteur et de leur territoire respectifs. Ces équipes effectuent un examen critique indépendant et exercent une surveillance afin d'assurer la qualité et la fidélité des modèles.

Les organisations dotées de ces équipes et de ces cadres doivent se poser les questions suivantes :

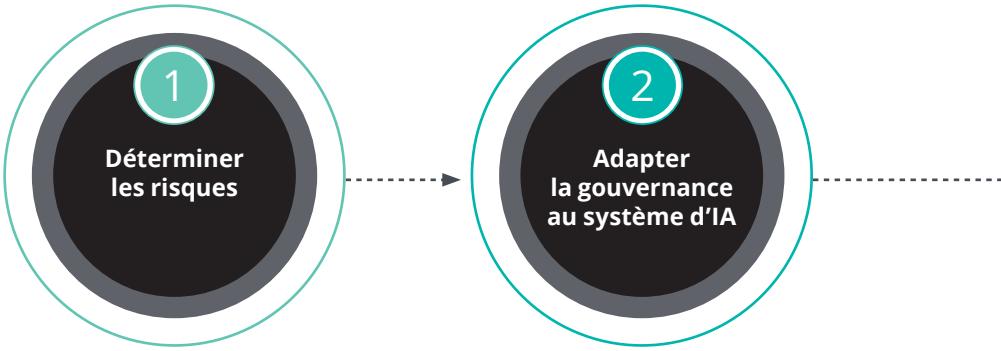
- Dans quelle mesure les capacités existantes des équipes de gestion des risques liés aux modèles et de validation des modèles devraient-elles être étendues à l'apprentissage machine et à d'autres technologies d'IA?
- La portée actuelle de la validation de modèles devrait-elle être revue pour assurer l'examen approprié des modèles d'IA de façon à inclure les outils intégrés, voire la validation appropriée des outils intégrés?
- Quels sous-ensembles des systèmes d'IA doivent faire l'objet de la validation la plus rigoureuse (p. ex., une validation indépendante très structurée)? Comment les autres systèmes d'IA seront-ils validés (p. ex., validation par les pairs, examen des processus et des décisions, autoévaluation)?
- Les équipes existantes devraient-elles s'en tenir à l'examen de la fiabilité et de la robustesse du système, ou étendre leur champ d'action à d'autres facteurs de risque inhérents à l'IA (p. ex., l'équité et l'impartialité)?

Les organisations n'ayant pas de fonction d'examen critique indépendant doivent envisager la façon dont les systèmes d'IA peuvent être adéquatement approuvés avant leur déploiement. Elles devraient tenir compte de la mesure dans laquelle les responsables de la validation sont indépendants des développeurs de système d'IA.

Le cadre de l'IA de confiance de Deloitte décrit ce qui constitue un modèle efficace de responsabilisation en matière d'IA, y compris les structures de gouvernance, les forums décisionnels et les responsabilités accrues du centre d'excellence en IA. Il fait aussi la lumière sur la participation des différentes parties prenantes dans le développement et le déploiement des systèmes d'IA.

Stratégies pour opérationnaliser la gouvernance

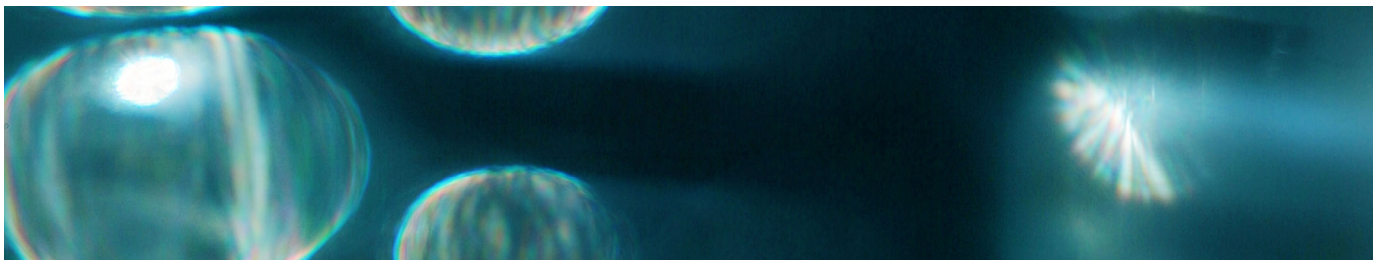
Une gouvernance efficace de l'IA de confiance est opérationnalisée en fonction des trois aspects suivants : les gens, les processus et les technologies. Après avoir abordé la responsabilisation, portons maintenant notre attention sur les processus et les technologies qui permettent de développer et de déployer des systèmes d'IA de confiance.

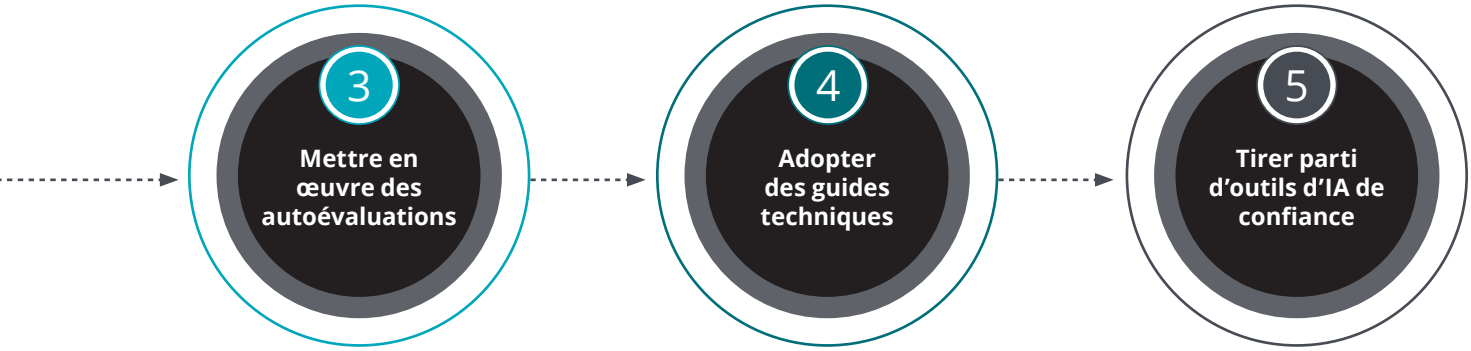


Les organisations doivent atteindre un équilibre entre l'utilisation accélérée de l'IA et la mise en place d'une gouvernance judicieuse de l'IA pour assurer sa fiabilité. Cinq stratégies essentielles s'offrent à elles :

Les organisations doivent déterminer les risques liés aux systèmes d'IA tôt au cours du cycle de vie. Cela permettra aux responsables et aux développeurs de système d'IA de prendre les bonnes décisions concernant la conception, le développement et le déploiement en vue d'instaurer la confiance, en plus de limiter les efforts consacrés à la reprise du développement. Parmi les pièges courants que peuvent entraîner l'évaluation et l'atténuation des risques au terme de l'étape du développement ou de la validation (assurance qualité), citons la nécessité de reprendre le travail, sans compter la perte de temps et d'investissements financiers si le projet ne peut être modifié et que, par conséquent, il ne peut être mis en œuvre.

La gestion des risques liés à l'IA mobilise un écosystème complexe d'intervenants, qui fournissent des directives et des stratégies d'atténuation en fonction de leur expertise fonctionnelle. Des experts dans les domaines de la confidentialité, de la conformité et de la sécurité, des scientifiques des données chevronnés, des éthiciens et des groupes interfonctionnels de leaders d'affaires jouent tous un rôle dans la gestion des risques liés à l'IA. Le responsable d'un système d'IA devrait être au courant des groupes de parties prenantes qu'il doit consulter pour assurer sa réussite et, par extension, les groupes auxquels il n'est pas nécessaire de faire appel étant donné les attributs du système d'IA. Cela exige une approche plus nuancée que dans le cas des niveaux de risque standard, qui peut être facilitée par une compréhension des principaux paramètres et attributs du système d'IA.





Les organisations dépendent grandement des responsables et des développeurs de systèmes d'IA pour déterminer les risques et adapter la gouvernance. Pour qu'il soit possible d'extraire la bonne quantité de renseignements, Deloitte a créé une autoévaluation de l'IA de confiance. Entre autres fonctions, cet outil recueille les paramètres clés du système d'IA pour évaluer les risques liés à l'IA qui nécessitent une attention et une analyse plus poussées, pour ensuite :

- Fournir des directives concrètes aux responsables et aux développeurs des systèmes d'IA afin d'éclairer leurs décisions de conception et de développement;
- Aiguiller les responsables des systèmes d'IA vers les experts (groupes ou fonctions) qu'ils doivent mobiliser pour gérer ces risques;

Cet outil soutient également l'inventaire des systèmes d'IA et la production de rapports regroupés afin de permettre à l'organisation de mieux comprendre en quoi consistent l'adoption de l'IA, le RCI et le profil de risque global, entre autres renseignements pertinents.

Les guides techniques fournissent aux développeurs de systèmes d'IA des directives tactiques propres à la situation. Ils visent les systèmes d'IA les plus courants au sein de l'organisation. Les guides stratégiques démontrent comment certaines techniques sont appliquées, et font référence à des outils et ressources libres ou acquis. Ils présentent aussi des techniques qui ont été testées et qui devraient avoir une longue vie utile, même s'ils doivent être révisés périodiquement à des fins de mises à jour des techniques, exemples et références.

Les guides stratégiques se prêtent particulièrement bien aux risques en matière d'équité et de caractère explicable, car leur atténuation s'applique au niveau du système d'IA individuel et nécessite souvent des méthodes techniques.

Deloitte a créé des guides stratégiques sur l'équité et le caractère explicable portant sur les types de systèmes d'IA que ses propres clients développent et déploient. Même si ceux-ci ne remplacent pas un solide programme de formation, il s'agit néanmoins de ressources essentielles pour les développeurs de systèmes d'IA.

Une fois que les responsables et les développeurs des systèmes d'IA ont utilisé l'autoévaluation pour dégager les risques liés à l'IA et prendre des décisions de conception éclairées, et qu'ils ont consulté les guides stratégiques techniques pour comprendre les mesures à prendre à un niveau détaillé, ils auront besoin d'outils logiciels pour améliorer leur système d'IA. Il peut s'agir de solutions libres ou acquises, conçues pour gérer les facteurs de risque tels que l'équité, le caractère explicable et la robustesse. Tandis que les organisations évaluent les coûts et les avantages de la création par rapport à l'acquisition de solutions, elles devront bien comprendre le contexte des logiciels, notamment les coûts réels, la personnalisation et le niveau de maîtrise nécessaire pour tirer efficacement parti des outils.

Deloitte a aussi bien analysé le contexte des outils d'IA de confiance et a créé des outils d'IA de confiance qui tiennent compte des facteurs de risque liés à l'IA.

Gestion du changement pour opérationnaliser la gouvernance

À mesure que les organisations adoptent l'IA, elles comprennent que celle-ci peut se traduire par d'importants changements transformationnels liés à la main-d'œuvre. Aussi, elles doivent se doter de stratégies de gestion du changement organisationnel afin d'appliquer une approche structurée à la transition vers l'état futur souhaité. Les entreprises devraient présenter leur point de vue sur l'IA de confiance dans leurs communications et inclure les considérations relatives à la gouvernance de l'IA dans l'orientation et la formation des employés.

Communications

Il sera essentiel de mettre en place une stratégie exhaustive de communication des politiques et des stratégies d'atténuation des risques de l'organisation pour démontrer un engagement envers les pratiques responsables d'IA.

Les communications devraient être adaptées aux différents publics cibles, aussi bien à l'externe qu'à l'interne.

- ***Parties prenantes externes telles que les utilisateurs, les clients, les actionnaires et le public :*** les organisations doivent énoncer clairement leur engagement à utiliser l'IA de manière responsable, notamment en faisant preuve de transparence en ce qui concerne les principes ou les politiques qu'elles respecteront.
- ***Parties prenantes internes telles que les employés, la haute direction et les membres du conseil d'administration :*** les communications doivent être claires et présenter des détails au sujet des processus et procédures internes. Les parties prenantes internes doivent comprendre leur rôle et leurs responsabilités envers l'atténuation des risques.

Éducation et formation

Outre des communications claires, une éducation et une formation peuvent être offertes à différents groupes de parties prenantes afin de les préparer à contribuer aux objectifs d'IA responsable de l'organisation.

Dirigeants et membres du conseil

- Les leaders doivent être mobilisés dès le début et souvent par la suite, et disposer des ressources nécessaires pour être en mesure de comprendre la prise de décisions stratégiques sur l'atténuation des risques d'affaires et inhérents à l'IA, et de prendre part à ces décisions.
- Les conseils d'administration doivent comprendre les risques que l'IA présente pour l'organisation et les activités de gouvernance qui permettent d'atténuer ces risques. Ils devraient être conscients des questions qu'ils doivent poser au sujet de l'IA.

Employés qui créent des systèmes d'IA

- L'éducation des développeurs doit être axée sur la sensibilisation des employés à l'égard des risques inhérents à l'IA et des risques d'affaires potentiels. Les employés doivent être en mesure d'utiliser les guides stratégiques techniques de l'organisation pour veiller à ce que les systèmes soient développés en fonction de l'engagement de l'organisation envers l'IA responsable.

Employés qui travaillent directement avec les systèmes d'IA

- Tandis que l'adoption de l'IA vient modifier les rôles et responsabilités, les employés qui travaillent directement avec les systèmes d'IA doivent bénéficier de la formation et des outils appropriés pour gérer les attentes émergentes.
- L'éducation devrait porter sur la sensibilisation aux risques liés aux systèmes d'IA, aux limites et aux hypothèses afin d'aider le personnel à prendre de meilleures décisions relatives à l'IA. Cela comprend la formation de certains employés pour leur permettre de comprendre les protocoles d'atténuation et de pouvoir les exécuter au moment opportun, s'il y a lieu.

Gestionnaires

- Les directeurs et chefs d'équipe doivent comprendre les conséquences que les systèmes d'IA et les risques liés à l'IA pourraient avoir sur leurs équipes afin d'être en mesure de les aider à prospérer.
- Les directeurs et chefs d'équipe doivent aussi avoir une excellente compréhension des structures de gouvernance et des rapports de responsabilité, et être en mesure de répartir efficacement les incidents à risque comme il se doit.

Organisation en général

- Toute formation de sensibilisation à l'IA qui s'adresse à un public général au sein de l'organisation devrait aussi comporter un volet d'éducation sur les risques liés à l'IA et l'engagement de l'organisation à les atténuer.

Dans le cadre de notre collaboration avec les clients qui entreprennent un parcours de transformation de l'IA, nous avons élaboré un programme et animé des séances de formation sur les risques et la gouvernance liés à l'IA adaptées à différents publics cibles.

Ces séances interactives sont offertes par l'intermédiaire de l'Académie d'IA de Deloitte, et peuvent avoir lieu en personne et en ligne. Ces académies s'adressent aux cadres dirigeants, aux leaders d'affaires ou aux leaders de la gestion des risques qui participent au développement de systèmes d'IA, ainsi qu'aux professionnels qui exécutent des initiatives d'affaires et techniques.

Personne-ressource

Preeti Shivpuri
Leader, Données et gouvernance de l'IA
Omnia IA
pshivpuri@deloitte.ca

Collaborateurs

Nira Sivakumar
Leader, Stratégie, Omnia IA

Michael Vinelli
Directeur, Omnia IA

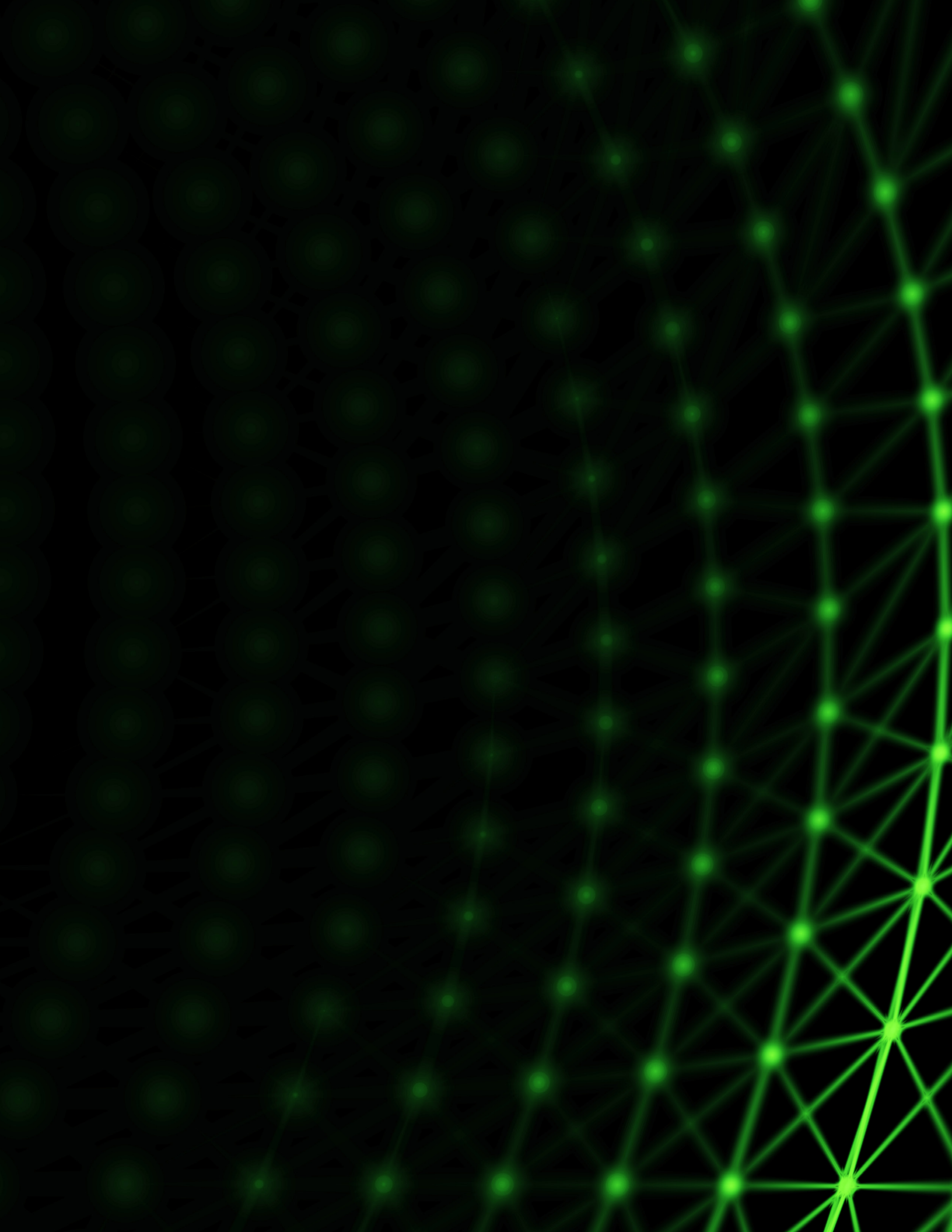
Amandeep Singh
Directeur, Omnia IA

Monika Viktorova
Consultante, Omnia IA

Remerciements

Ishani Majumdar
Directrice, Services financiers, Consultation

Denizhan Uykur
Conseiller principal, Monitor Deloitte



www.deloitte.ca

À propos de Deloitte
Deloitte offre des services dans les domaines de l'audit et de la certification, de la consultation, des conseils financiers, des conseils en gestion des risques, de la fiscalité et d'autres services connexes à de nombreuses sociétés ouvertes et fermées dans différents secteurs. Deloitte sert quatre entreprises sur cinq du palmarès Fortune Global 500^{MD} par l'intermédiaire de son réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offre les compétences de renommée mondiale, le savoir et les services dont les clients ont besoin pour surmonter les défis d'entreprise les plus complexes. Deloitte S.E.N.C.R.L./s.r.l., société à responsabilité limitée constituée en vertu des lois de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres, voir www.deloitte.com/ca/apropos.

Notre raison d'être mondiale est d'avoir une influence marquante. Chez Deloitte Canada, cela se traduit par la création d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons concrétiser cette raison d'être en incarnant nos valeurs communes qui sont d'ouvrir la voie, de servir avec intégrité, de prendre soin les uns des autres, de favoriser l'inclusion et de collaborer pour avoir une influence mesurable.

Pour en apprendre davantage sur les quelque 312 000 professionnels de Deloitte, dont plus de 12 000 font partie du cabinet canadien, veuillez nous suivre sur LinkedIn, Twitter, Instagram ou Facebook.

Conçu et produit par L'Agence| Deloitte Canada. 20-3287597T