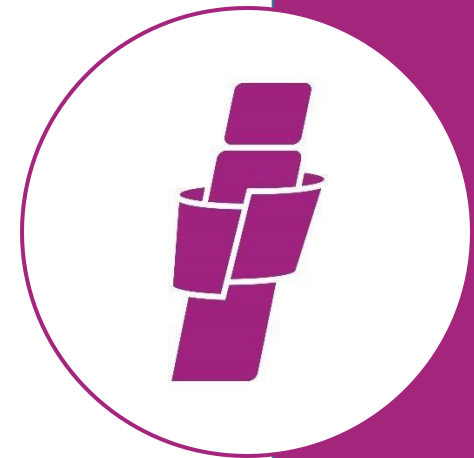
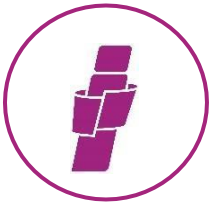


# Directives en matière de gouvernance de l'IA

**Phase 1** - Groupe de travail sur l'intelligence artificielle de l'ACAC



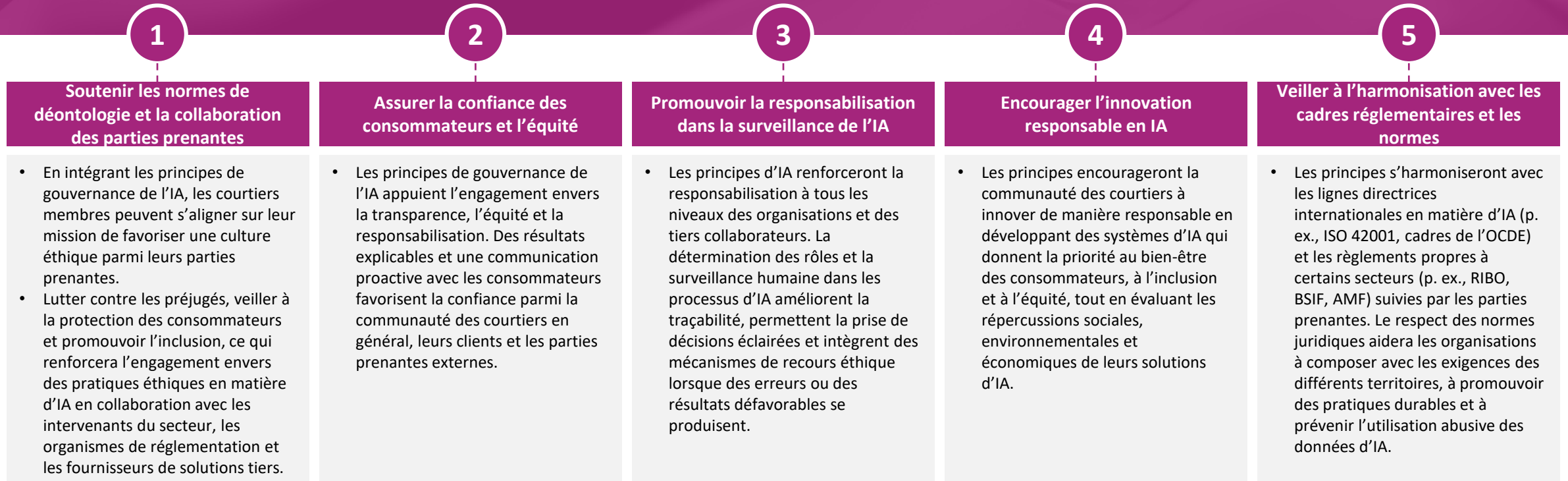


# Table des matières

| Sections |   | Page      |
|----------|---|-----------|
| 01       | Objectifs des principes directeurs de l'IA                              | <u>03</u> |
| 02       | Méthode   | <u>04</u> |
| 03       | Sommaire des thèmes principaux fondés sur les renseignements sectoriels | <u>05</u> |
| 04       | Principes directeurs de l'IA pour la communauté des courtiers           | <u>07</u> |
| 05       | Mise en œuvre des principes directeurs de l'IA                          | <u>08</u> |
| 06       | Autres considérations – Programme de gouvernance de l'IA                | <u>09</u> |
| 07       | Annexe  | <u>12</u> |

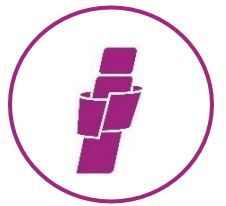


# Les principes directeurs de l'IA sont conçus pour aider la communauté des courtiers à atteindre les cinq objectifs suivants



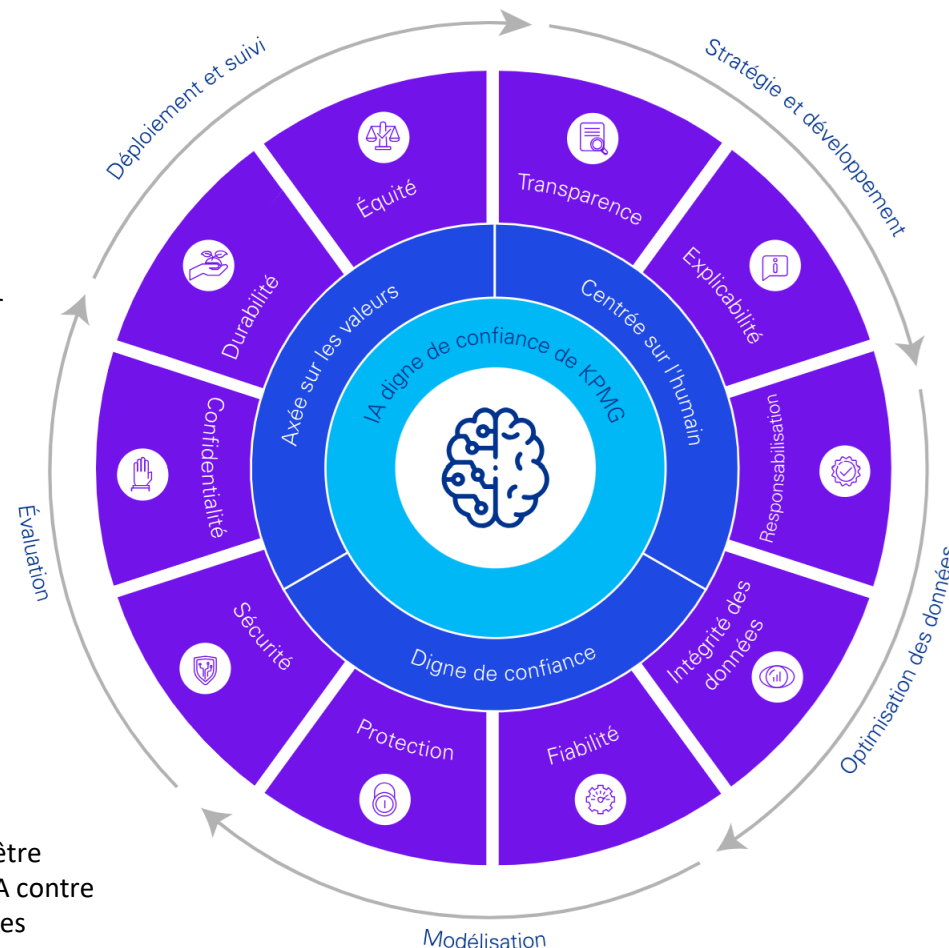
## Les principes d'IA offrent également les avantages suivants à la communauté des courtiers :

- Promouvoir une compréhension unifiée du rôle de l'IA au sein de la communauté des courtiers
- Orienter les pratiques de gestion des risques, les structures de gouvernance et les processus décisionnels pour l'utilisation de l'IA dans les cabinets
- Fournir aux équipes de courtiers des directives pratiques et exploitables à intégrer à toutes les phases du développement de l'IA, y compris la conception, la validation, le déploiement et la surveillance
- Améliorer la collaboration interfonctionnelle entre les courtiers, les organismes de réglementation, les groupes sectoriels, les fournisseurs de technologie et les associations membres en mettant de l'avant des objectifs communs et un langage commun pour aborder les sujets liés à l'IA

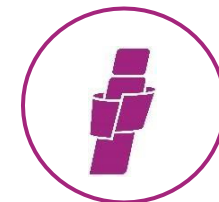


# Le cadre d'IA de confiance de KPMG a servi de fondement à l'élaboration des principes directeurs de l'IA

- Équité**  
 Les solutions d'IA doivent être conçues pour réduire ou éliminer les préjugés contre les personnes, les communautés et les groupes.
- Durabilité**  
 Les solutions d'IA doivent être conçues de manière à utiliser efficacement l'énergie, à réduire les émissions de carbone et à soutenir un environnement plus sain.
- Confidentialité**  
 Les solutions d'IA doivent se conformer aux lois et aux règles de protection de la vie privée et des données en vigueur.
- Sécurité**  
 Les solutions d'IA doivent être conçues et mises en œuvre pour protéger les personnes, les entreprises et la propriété contre les dommages.
- Protection**  
 Des pratiques robustes et résilientes doivent être mises en place pour protéger les solutions d'IA contre les acteurs malveillants, la désinformation et les événements indésirables.



- Transparence**  
 Les solutions d'IA doivent comprendre des divulgations responsables pour que les parties prenantes comprennent bien ce qui se passe à chaque étape du cycle de vie de l'IA.
- Explicabilité**  
 Les solutions d'IA doivent être conçues et livrées avec toutes les réponses aux questions sur les façons et les raisons d'arriver à une conclusion.
- Responsabilisation**  
 La surveillance et la responsabilité humaines doivent être intégrées au cycle de vie de l'IA pour gérer les risques et assurer la conformité aux lois et règles en vigueur.
- Intégrité des données**  
 Les données utilisées dans les solutions d'IA doivent être acquises conformément aux lois et aux règles applicables; leur exactitude, leur exhaustivité, leur pertinence et leur qualité doivent être évaluées afin de favoriser la prise de décisions éclairées.
- Fiabilité**  
 Les solutions d'IA doivent en tout temps être utilisées conformément à la portée et à l'objectif prévus ainsi qu'au degré de précision souhaité.



## Des analyses sectorielles consolidées ont mis en évidence des thèmes principaux communs dont découlent les principes directeurs de l'IA (1/2)

| Thèmes principaux                                 |               |  |                                     |                                     |                                     |                                       |   |  |                                     |                                       |                                     |
|---|---------------|--|-------------------------------------|-------------------------------------|-------------------------------------|---------------------------------------|---|--|-------------------------------------|---------------------------------------|-------------------------------------|
|   | 1             | 2  | 3                                   | 4                                   | 5                                   | 6                                     | 7   | 8  | 9                                   | 10                                    | 11                                  |
|   | Collaboration | Efficacité et amélioration des services fondées sur l'IA | Protection des consommateurs        | Gestion des risques                 | Maintien des liens personnels       | Exactitude et gouvernance des données | Conformité à la réglementation et codes de conduite | Déontologie et utilisation responsable de l'IA | Formation et surveillance humaine   | Impact et durabilité environnementale | Gouvernance et responsabilité       |
| Directives propres à certains secteurs d'activité | RIBO          | <input checked="" type="checkbox"/>                      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/>   | <input checked="" type="checkbox"/>                 | <input checked="" type="checkbox"/>            | <input checked="" type="checkbox"/> |                                       |                                     |
|   | AMF           |  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     |                                       | <input checked="" type="checkbox"/>                 | <input checked="" type="checkbox"/>            |                                     |                                       | <input checked="" type="checkbox"/> |
|   | BSIF          | <input checked="" type="checkbox"/>                      |                                     | <input checked="" type="checkbox"/> |                                     |                                       | <input checked="" type="checkbox"/>                 |  |                                     |                                       |                                     |
|   | BIBA          | <input checked="" type="checkbox"/>                      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                                     | <input checked="" type="checkbox"/>   | <input checked="" type="checkbox"/>                 |  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/>   |                                     |
|   | OCDE          |  |                                     |                                     |                                     |                                       |   |  |                                     | <input checked="" type="checkbox"/>   | <input checked="" type="checkbox"/> |
|   | IAIS          |  |                                     | <input checked="" type="checkbox"/> |                                     |                                       |   |  |                                     |                                       | <input checked="" type="checkbox"/> |
|   | ABI           |  |                                     | <input checked="" type="checkbox"/> |                                     | <input checked="" type="checkbox"/>   | <input checked="" type="checkbox"/>                 | <input checked="" type="checkbox"/>            |                                     |                                       | <input checked="" type="checkbox"/> |

**RIBO** : Registered Insurance Brokers of Ontario, **AMF** : Autorité des marchés financiers, **BSIF** : Bureau du surintendant des institutions financières, **BIBA** : The British Insurance Brokers' Association, **OCDE** : Organisation de coopération et de développement économiques, **IAIS** : International Association of Insurance Supervisors, **ABI** : Association of British Insurers

Les thèmes ne correspondent pas toujours directement à toutes les directives sectorielles. Veuillez consulter l'annexe pour obtenir un résumé des directives de chaque secteur d'activité.

## Directives propres à certains secteurs d'activité

**RIBO** : Registered Insurance Brokers of Ontario, **AMF** : Autorité des marchés financiers, **BSIF** : Bureau du surintendant des institutions financières, **BIBA** : The British Insurance Brokers' Association, **OCDE** : Organisation de coopération et de développement économiques, **IAIS** : International Association of Insurance Supervisors, **ABI** : Association of British Insurers

6



En nous appuyant sur le cadre et les connaissances de premier plan du secteur, nous avons élaboré sept principes directeurs de l'IA qui cadrent avec les valeurs de l'ACAC

Valeurs de l'ACAC

1. Protection des consommateurs

2. Collaboration

3. Leadership

4. Durabilité

5. Représentation

6. Engagement envers la collectivité

7. Innovation et technologie

8. Perfectionnement professionnel

Principes directeurs de l'IA



### 1. Sûreté, sécurité et fiabilité

Les solutions d'IA sont conçues et mises en œuvre à l'aide de **pratiques robustes et résilientes** qui protègent contre les **menaces, les acteurs malveillants, la désinformation et les événements indésirables**, assurent la sécurité de toutes les parties prenantes et fonctionnent constamment aux niveaux de précision souhaités



### 2. Respect de la vie privée et intégrité des données

Les solutions d'IA et les données utilisées sont conçues et acquises **conformément aux lois et aux règles en vigueur**; leur **exactitude**, leur **exhaustivité**, leur **pertinence** et leur **qualité** doivent être évaluées afin de **favoriser la prise de décisions éclairées**



### 3. Explicabilité et transparence

**Divulgations et conception responsables** qui répondent aux **questions de savoir** comment et **pourquoi une conclusion a été tirée d'une solution d'IA**, en veillant à ce que les parties prenantes comprennent ce qui se passe dans le cycle de vie de l'IA



### 4. Équité

Les solutions d'IA assurent une **prise de décision impartiale** pour favoriser la **confiance** et la **collaboration** entre les courtiers, les organismes de réglementation, les groupes sectoriels, les fournisseurs de technologie et les associations membres



### 5. Durabilité

Les solutions d'IA contribuent à assurer un **avenir dynamique** et à **long terme** pour le **réseau de distribution des courtiers**



### 6. Responsabilisation et relations humaines

Les solutions d'IA assurent la **surveillance** et la **responsabilité humaines** d'être responsable envers les clients de la protection de leurs intérêts, de la gestion des risques et de la **conformité aux lois et règlements en vigueur**



### 7. Efficacité et service à la clientèle fondés sur l'IA

Optimiser les flux de travail grâce à des solutions d'IA pour **améliorer le traitement des demandes** et la **souscription**, tout en adaptant les solutions grâce à l'**analyse prédictive**. Veiller à préserver la **surveillance humaine** pour le traitement des cas complexes



## Plan de mise en œuvre des principes directeurs de l'IA pour favoriser l'adoption sécuritaire de l'IA dans la communauté des courtiers

Où nous en sommes maintenant : Élaboration de principes directeurs de l'IA, à partir des connaissances sectorielles et des pratiques exemplaires, pour aider les courtiers à adopter l'IA de façon responsable

Prochaines étapes pour la communauté des courtiers : appliquer les principes directeurs pour assurer l'adoption sécuritaire des solutions d'IA

### Communiquer

L'ACAC communique les principes directeurs définitifs de l'IA à la communauté des courtiers par les voies appropriées

### Approuver

Les courtiers devraient examiner l'ébauche des principes directeurs aux fins de validation, de modification et d'approbation

### Mettre en œuvre

Les courtiers devraient intégrer les principes directeurs dans les processus existants - par exemple, les évaluations des risques, les évaluations des risques liés aux fournisseurs et la formation

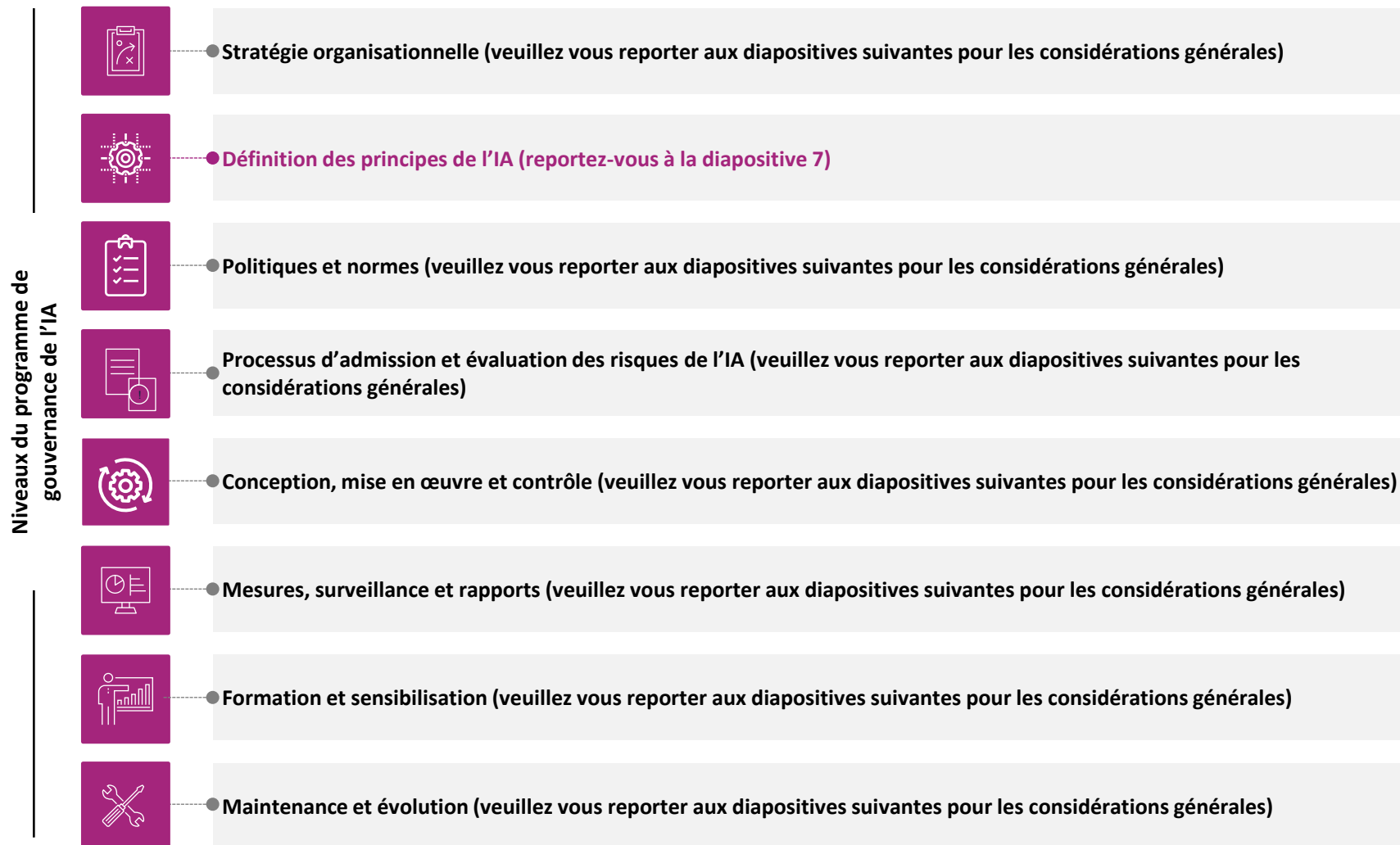
### Mettre à jour

Les courtiers devraient continuer de mettre à jour les principes directeurs de l'IA en fonction de l'évolution de la réglementation, des capacités d'IA et des attentes des parties prenantes. Leur révision annuelle est considérée comme une pratique exemplaire

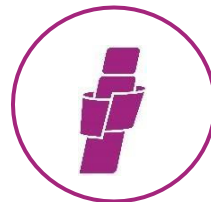




## Résumé des considérations générales pour les sept autres niveaux du programme de gouvernance de l'IA



- La définition des principes de l'IA est une première étape essentielle pour jeter les bases d'une approche de gestion des risques axée sur l'utilisateur final. Les principes directeurs assurent l'harmonisation des responsabilités et des limites déontologiques dans lesquelles les systèmes d'IA devraient fonctionner.
- Pour les sept autres niveaux du programme de gouvernance de l'IA, des considérations générales sur la stratégie, les risques, la conformité et l'habilitation opérationnelle sont présentées dans les diapositives suivantes.



# Considérations relatives aux autres niveaux de gouvernance de l'IA – Partie 1

## 1. Stratégie organisationnelle

- Une stratégie d'IA aligne les **objectifs commerciaux** sur un cadre de gouvernance qui intègre la déontologie, la gestion des risques et la conformité à **toutes les étapes du cycle de vie de l'IA, du développement au déploiement**
- Elle établit des **objectifs commerciaux** et un **cadre évolutif** pour tirer parti de la technologie de l'IA en décrivant les **indicateurs de rendement clés**, les **contrôles internes**, les **programmes de formation** et les **mécanismes de rétroaction continue**. Cette **approche** s'adapte aux changements réglementaires et technologiques, en veillant à ce que l'IA soit intégrée efficacement et gérée de manière responsable afin d'atténuer les **risques opérationnels, déontologiques et juridiques**

## 2. Politiques et normes

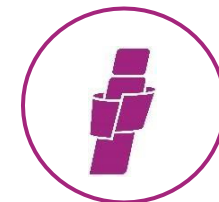
- Un **cadre efficace de politiques et de normes en IA** devrait définir des lignes directrices opérationnelles, déontologiques et réglementaires
- Une bibliothèque de règles devrait fournir des conseils sur l'ensemble du **cycle de vie du modèle d'IA**, de la conception à la surveillance après déploiement, pour assurer la confiance et la responsabilité
- En établissant des **rôles**, des **mesures de rendement** et des **protocoles de gestion du changement clairs**, les organisations peuvent s'assurer que tous les systèmes d'IA fonctionnent conformément aux **pratiques exemplaires internes** et aux **exigences réglementaires externes**. Cette approche favorise la transparence, la responsabilisation et la confiance tout au long du cycle de vie de l'IA
- Élaborer et améliorer les politiques - les principales politiques à prendre en considération comprennent :
  - Politique de gouvernance de l'IA
  - Politique d'utilisation acceptable de l'IA
  - Politique en matière de protection des renseignements personnels
  - Politique de gestion des données
  - Politique de gestion de la sécurité de l'information

## 3. Processus d'admission et évaluation des risques liés à l'IA

- Déployer un **questionnaire libre-service de triage des risques** qui évalue de façon cohérente les nouveaux cas d'utilisation de l'IA. Ce processus de prise en charge devrait saisir les **détails clés** dès le départ - dépendances des modèles, qualité des données, considérations déontologiques et fonctionnalité voulue - afin d'établir un **parcours de gouvernance des risques adapté** à chaque solution d'IA
- Le **processus d'évaluation des risques** devrait être conforme aux **principes, aux politiques et aux normes établis en matière d'IA**. Les principales composantes comprennent une documentation exhaustive, une surveillance continue et des réévaluations périodiques visant à identifier et à atténuer les risques opérationnels, déontologiques et réglementaires potentiels. La gestion précoce des risques permet de s'assurer qu'ils sont gérés conformément à la **propension au risque** et aux **exigences de conformité** de l'organisation
- Le processus devrait s'appuyer sur une **plateforme technologique** évolutive (p. ex., PowerApps), qui facilite le suivi, la production de rapports et l'examen périodique des initiatives d'IA

## 4. Formation et sensibilisation

- Effectuer l'**évaluation des besoins d'apprentissage** afin de déployer un programme de formation à l'échelle de l'entité qui établit une **compréhension de base des principes fondamentaux de l'IA**, y compris ses risques, les considérations déontologiques et l'utilisation responsable, tout en offrant une **formation propre à chaque rôle** pour les différentes lignes de défense et de leadership. La formation devrait permettre à **tous les employés** - non seulement ceux qui occupent des postes techniques, mais aussi ceux qui travaillent dans les domaines des risques, de la conformité et de l'exploitation - d'acquérir les connaissances nécessaires pour **gérer et atténuer les risques liés à l'IA**, en veillant à ce que chaque professionnel comprenne ses responsabilités en matière de **respect des normes déontologiques et de la réglementation**



## Considérations relatives aux autres niveaux de gouvernance de l'IA – Partie 2

### 5. Conception, mise en œuvre et contrôle

- Les processus de conception, de mise en œuvre et de contrôle favorisent un environnement d'utilisation éthique de l'IA et de transparence et font en sorte que les initiatives d'IA demeurent résilientes et conformes aux exigences opérationnelles et réglementaires
- **Conception** : Les organisations devraient établir des contrôles à l'égard des principaux secteurs de risque, en s'assurant que le cycle de vie de chaque système d'IA est planifié. Ces mesures devraient porter sur la qualité des données, la sécurité, l'utilisation éthique et la conformité réglementaire
- **Mise en œuvre** : Les contrôles de conception devraient être intégrés aux flux des travaux opérationnels au moyen de politiques clairement documentées, de programmes de formation rigoureux et d'une mobilisation proactive des parties prenantes. Cette approche permet de s'assurer que chaque cas d'utilisation de l'IA cadre avec les principaux objectifs commerciaux et demeure adaptable aux risques et aux changements émergents
- **Contrôle** : Les organisations doivent suivre et évaluer l'efficacité des contrôles établis pour gérer les risques liés à l'IA et assurer la conformité tout au long du cycle de vie du système d'IA

### 6. Mesures, surveillance et rapports

- S'assurer que les systèmes d'IA demeurent **conformes** aux **normes déontologiques et réglementaires** et que tout écart est rapidement corrigé au moyen de stratégies de correction éclairées
- Le cadre de référence pour les mesures, la surveillance et les rapports définit des **paramètres clairs et mesurables** pour évaluer les risques et la performance liés à l'IA, tant au niveau de l'organisation que du déploiement. Ce cadre exige l'établissement d'**indicateurs clés de risque (ICR)** et d'**indicateurs clés de performance (ICP) normalisés** qui cadrent avec les objectifs stratégiques et fournissent une **méthode cohérente** pour **comparer, suivre et ajuster** les pratiques de gestion des **risques**, assurant ainsi une amélioration continue et une prise de décision efficace
- Déployer des **outils de surveillance en temps réel**, comme des systèmes de tableau de bord et des alertes en direct, pour **repérer rapidement les anomalies et les changements dans les profils de risque**, et mettre en œuvre des mécanismes de signalement rigoureux qui communiquent ces mesures à la direction en interne ainsi qu'aux organismes de réglementation en externe

### 7. Maintenance et évolution

- Adopter une approche dynamique et itérative qui **examine, met à jour et peaufine continuellement ses politiques et ses contrôles** afin de rester en phase avec les règlements émergents, les pratiques exemplaires du secteur et la croissance organisationnelle
- **Flux des travaux axés sur la technologie**, comme la gestion de l'inventaire des modèles, les processus de certification des modèles, la hiérarchisation automatisée des risques et le suivi des problèmes, et la surveillance régulière des tableaux de bord pour **saisir et traiter les problèmes de rendement et de conformité** des systèmes d'IA en temps réel
- Établir des **boucles de rétroaction claires** et des **audits périodiques** pour s'assurer que tout changement dans le contexte réglementaire ou technologique est rapidement intégré, tandis que les programmes de formation continue mettent à jour les compétences des employés et favorisent une **culture proactive de gestion des risques** pour maintenir et faire évoluer la **gouvernance de l'IA**, en veillant à ce que l'approche demeure agile et réactive à l'évolution de l'environnement de risque

# Annexe

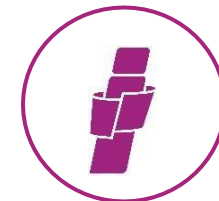




# RIBO - Exploration initiale de l'innovation en intelligence artificielle (IA) dans le secteur des courtiers d'assurance de dommages de l'Ontario

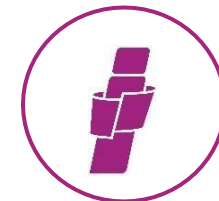
| Thèmes principaux  |  |
|--|--|
| <p><b>Collaboration</b></p> <ul style="list-style-type: none"> <li>Favoriser les partenariats avec les organismes de réglementation et d'autres organisations pour explorer les possibilités technologiques.</li> <li>Mener des efforts de recherche conjoints et partagés pour faire progresser les applications de l'IA.</li> </ul> <p><b>Traitement équitable des clients en assurance</b></p> <ul style="list-style-type: none"> <li>Établir de solides garde-fous pour s'assurer que l'évolution technologique s'harmonise avec le traitement équitable des consommateurs.</li> <li>Promouvoir des pratiques éthiques et veiller à ce que l'IA serve les intérêts des consommateurs.</li> </ul> <p><b>Efficacité et amélioration des services fondées sur l'IA</b></p> <ul style="list-style-type: none"> <li>Tirer parti de l'IA pour améliorer l'efficacité opérationnelle et offrir des services de grande qualité aux clients.</li> <li>Intégrer des outils d'IA pour les processus administratifs (p. ex., gestion des données, robots conversationnels) et les rôles en contact avec les consommateurs (p. ex., marketing, souscription, modélisation des risques).</li> </ul> <p><b>Protection des consommateurs</b></p> <ul style="list-style-type: none"> <li>Atténuation des risques de partialité, de discrimination et d'atteinte à la vie privée.</li> <li>Assurer la transparence, la responsabilisation et la confiance des consommateurs dans les systèmes d'IA.</li> </ul> <p><b>Maintien des liens personnels</b></p> <ul style="list-style-type: none"> <li>Préserver des relations courtiers-consommateurs significatives malgré l'adoption croissante de l'IA.</li> </ul> <p><b>Gestion des risques liés aux tiers</b></p> <p>Mettre en place des contrôles rigoureux pour gérer les risques associés aux fournisseurs d'IA tiers, notamment :</p> <ul style="list-style-type: none"> <li>Veiller à ce que les fournisseurs respectent les réglementations du secteur et les codes de conduite.</li> <li>Évaluer la façon dont les solutions tierces traitent la confidentialité et la sécurité des données.</li> <li>Effectuer un contrôle diligent des fournisseurs et comprendre les responsabilités en cas de résultats incorrects de l'IA.</li> </ul> | <p><b>Gestion des risques</b></p> <ul style="list-style-type: none"> <li>Relever les principaux défis, comme les biais dans les données, la réduction de la transparence, l'utilisation potentiellement abusive des données sur les consommateurs et l'explicabilité des résultats de l'IA pour les consommateurs.</li> <li>Accorder la priorité au consentement éclairé et veiller à ce que les courtiers puissent expliquer aux clients les recommandations fondées sur l'IA.</li> </ul> <p><b>Exactitude des données et gouvernance</b></p> <ul style="list-style-type: none"> <li>Effectuer des audits réguliers des modèles d'IA pour harmoniser les recommandations avec les besoins en évolution des clients.</li> <li>S'assurer que les données utilisées dans les systèmes d'IA sont exactes, impartiales et conformes aux exigences légales.</li> </ul> <p><b>Utilisation éthique et responsable de l'IA</b></p> <ul style="list-style-type: none"> <li>Établir des lignes directrices éthiques pour le marketing fondé sur l'IA afin de prioriser les avantages pour les consommateurs plutôt que les profits.</li> <li>Appliquer des politiques de gouvernance pour assurer le développement et le déploiement responsables des outils d'IA.</li> </ul> <p><b>Conformité à la réglementation et codes de déontologie</b></p> <ul style="list-style-type: none"> <li>Respecter la réglementation du secteur et le code de déontologie des courtiers, qui met l'accent sur l'honnêteté, la compétence, les intérêts des clients, la protection de la vie privée et la responsabilité.</li> <li>Harmoniser les solutions d'IA avec les normes juridiques et déontologiques.</li> </ul> <p><b>Formation et surveillance humaine</b></p> <ul style="list-style-type: none"> <li>Fournir aux courtiers la formation nécessaire pour comprendre et utiliser efficacement les systèmes d'IA.</li> <li>Maintenir l'intervention humaine pour superviser les conseils présentant des enjeux élevés et veiller à ce que les recommandations soient judicieuses et transparentes.</li> </ul> <p><b>Transparence des modèles d'IA et responsabilité</b></p> <ul style="list-style-type: none"> <li>S'attaquer à l'enjeu lié au fait que des courtiers ne sont pas en mesure d'expliquer les décisions générées par l'IA.</li> <li>Veiller à ce que des structures de responsabilité soient en place pour les erreurs découlant des modèles d'IA.</li> </ul> |





# AMF - Pratiques exemplaires pour l'utilisation responsable de l'IA dans le secteur financier

| Thèmes principaux  |   |
|--|---|
| <p><b>Transformation numérique et évolution du secteur</b></p> <ul style="list-style-type: none"> <li>Tirer parti des technologies d'IA pour favoriser la transformation numérique et améliorer l'efficacité, l'innovation et l'expérience client dans l'ensemble du secteur du courtage d'assurance.</li> </ul> <p><b>Conformité à la réglementation et protection des consommateurs</b></p> <ul style="list-style-type: none"> <li>Veiller au respect des lois, règlements et directives pertinents pour protéger les droits des consommateurs et respecter les exigences de conformité du secteur lors de l'adoption de l'IA.</li> </ul> <p><b>Utilisation responsable de l'IA</b></p> <ul style="list-style-type: none"> <li>Promouvoir des pratiques éthiques en matière d'IA, minimiser les préjudices, assurer l'équité et donner la priorité à la mise en œuvre ciblée et appropriée de l'IA.</li> </ul> <p><b>Transparence et reddition de comptes</b></p> <ul style="list-style-type: none"> <li>Relever les défis posés par les systèmes de « boîte noire » de l'IA en mettant en œuvre des modèles clairs et explicables et en justifiant l'utilisation de l'IA dans les produits et services.</li> <li>Établir une communication transparente avec les consommateurs, notamment en communiquant les cadres de conception de l'IA, en expliquant les résultats et en offrant de l'aide pour répondre aux demandes des consommateurs.</li> </ul> <p><b>Gestion de la dérive des modèles</b></p> <ul style="list-style-type: none"> <li>Surveiller la dérive des modèles et s'y adapter - les changements dans la performance de l'IA en raison des nouvelles données - pour assurer une fiabilité continue et l'harmonisation avec les besoins des entreprises ou des consommateurs.</li> </ul> <p><b>Cybersécurité et protection des renseignements personnels</b></p> <ul style="list-style-type: none"> <li>Atténuer les risques liés aux données à caractère personnel et prendre des mesures de cybersécurité rigoureuses pour protéger les renseignements sensibles des consommateurs contre les cyberattaques.</li> </ul> <p><b>Protection des consommateurs et confiance</b></p> <ul style="list-style-type: none"> <li>Développer des solutions d'IA qui agissent dans l'intérêt des consommateurs, respectent la vie privée, préservent la liberté de choix et traitent les consommateurs équitablement.</li> <li>Gérer les conflits d'intérêts et consulter les consommateurs concernant l'adoption de l'IA, en favorisant l'autonomie et la confiance dans les services fondés sur l'IA.</li> </ul> | <p><b>Transparence de l'utilisation de l'IA auprès des consommateurs</b></p> <ul style="list-style-type: none"> <li>Donner des détails sur la conception et l'utilisation du système d'IA, tout en guidant les consommateurs à travers les résultats générés par l'IA et en leur offrant des possibilités d'assistance.</li> <li>Prendre des décisions claires et faciles à expliquer, en veillant à ce que les avantages l'emportent sur les risques potentiels.</li> </ul> <p><b>Éthique et responsabilité dans la conception et l'exploitation de l'IA</b></p> <ul style="list-style-type: none"> <li>Adopter un code d'éthique pour guider le développement et la mise en œuvre de l'IA, en mettant l'accent sur la transparence et l'intégrité éthique.</li> <li>Responsabiliser la direction, les employés et les cadres dirigeants à l'égard des décisions liées à l'IA, en veillant à la surveillance humaine des répercussions importantes sur les consommateurs.</li> </ul> <p><b>Pratiques exemplaires en matière de conception, de déploiement et de surveillance de l'IA</b></p> <ul style="list-style-type: none"> <li>Favoriser une culture d'inclusion et d'éthique qui permet de signaler les erreurs et de dénoncer les abus sans représailles.</li> <li>Former des équipes diversifiées et bien formées qui travaillent sur des projets d'IA.</li> <li>Assurer un processus uniforme pour la conception, la mise en œuvre et la surveillance des systèmes d'IA, y compris le contrôle diligent des solutions d'IA tierces.</li> <li>Relier les initiatives d'IA aux objectifs durables en matière de pratiques commerciales responsables sur le plan environnemental et social.</li> </ul> <p><b>Gestion des risques et gouvernance pour les solutions d'IA</b></p> <ul style="list-style-type: none"> <li>Évaluer les risques liés aux solutions d'IA en termes de complexité, d'incidence et de sécurité, en remédiant aux vulnérabilités et en assurant une protection robuste contre les menaces à la cybersécurité.</li> <li>Régir l'utilisation des données avec soin, en veillant à la fiabilité, au traitement éthique des données de tiers et synthétiques et à leur anonymisation appropriée, au besoin.</li> <li>Mener des évaluations des risques rigoureuses à chaque étape du cycle de vie de l'IA, effectuer des analyses d'impact algorithmiques et tester l'IA dans des environnements contrôlés avant son déploiement.</li> <li>Maintenir la surveillance, l'audit et la formation des employés en continu pour atténuer les risques, évaluer la performance de l'IA et préserver la fiabilité au fil du temps.</li> </ul> |



# BSIF et ACFC - Utilisations et risques de l'IA dans les institutions financières fédérales

## Thèmes principaux

### Gestion des risques liés à l'IA

- Gérer les risques internes liés à l'utilisation de solutions d'IA et les risques externes liés à des tiers, y compris les pirates qui exploitent l'IA générative à des fins malveillantes.
- Mener des évaluations périodiques pour identifier et atténuer les risques associés au déploiement de l'IA.

### Applications de l'IA

- Amélioration de l'efficacité opérationnelle.
- Identification et atténuation des risques.
- Détection de la fraude et cybersécurité (p. ex. détection des anomalies de réseau, des hameçonnages).
- Mesures visant à améliorer la confidentialité et la sécurité des données.
- Engagement client (p. ex. robots conversationnels, conseils financiers personnalisés, vérification de la relation client).
- Gestion du risque lié aux modèles (p. ex. apprentissage autonome des données, harmonisation des données d'entrée et de sortie).

### Gouvernance des données et conformité réglementaire :

Lutter contre les défis liés aux éléments suivants :

- Confidentialité des données et propriété fragmentée des données.
- Exigences réglementaires et conformité des territoires.
- Assurance de la qualité des données et supervision des ententes relatives aux données de tiers.

### Considérations relatives aux modèles d'IA :

- Élaborer des modèles explicables, transparents et impartiaux.
- Favoriser la collaboration entre les utilisateurs, les développeurs et les fonctions de contrôle lors de la conception et de la mise en œuvre.
- Gérer les risques liés aux modèles, y compris l'apprentissage autonome, les défis liés aux paramètres et les relations entre les données d'entrée et de sortie.

### Risques liés aux fournisseurs tiers :

- Évaluer et atténuer les risques liés à la dépendance, comme les risques de concentration avec les grands fournisseurs de technologie.
- Veiller au respect de la réglementation et maintenir des mesures de sécurité des données rigoureuses pour l'utilisation du nuage.

### Risques opérationnels, juridiques et liés à la cybersécurité :

- Aborder les systèmes interconnectés et la complexité des données qui peuvent menacer la résilience opérationnelle.
- Anticiper les dysfonctionnements de l'IA ayant des répercussions potentielles sur les finances ou la réputation.
- Surveiller les risques juridiques, déontologiques et de réputation liés à la confidentialité et au consentement des consommateurs.

### Collaboration :

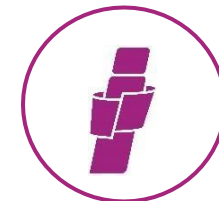
- Collaborer avec les organismes de réglementation, les organismes gouvernementaux et les ministères pertinents pour mieux gérer les risques propres à l'IA.

### IA responsable et fiable :

- Plaider en faveur des technologies d'IA générative qui privilégient la confidentialité, la responsabilité et l'utilisation éthique.

### Éducation et élaboration de stratégies :

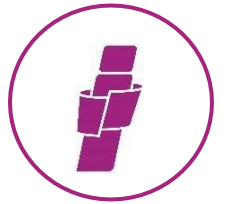
- Offrir de la formation aux employés sur les solutions d'IA et les risques connexes.
- Établir une stratégie d'IA globale tenant compte de l'interdépendance avec les systèmes, les données et les risques d'entreprise.



## British Insurance Broker's Association (BIBA) - Guide sur l'IA

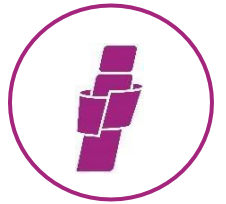
| Thèmes principaux   |  |
|---|--|
| <p><b>Efficacité et amélioration des services fondés sur l'IA</b></p> <ul style="list-style-type: none"> <li>Tirer parti des solutions fondées sur l'IA pour rationaliser les opérations administratives (comme la gestion des données et le traitement automatisé des documents) et les fonctions en contact avec les consommateurs comme la souscription et le traitement des demandes, améliorant ainsi l'efficacité opérationnelle globale et l'expérience client.</li> </ul> <p><b>Conformité à la réglementation et codes de conduite</b></p> <ul style="list-style-type: none"> <li>Veiller au strict respect des cadres réglementaires et des codes internes en alignant la mise en œuvre de l'IA sur les exigences juridiques et les normes du secteur.</li> </ul> <p><b>Gestion des risques, responsabilité et protection des consommateurs</b></p> <ul style="list-style-type: none"> <li>Adopter des pratiques rigoureuses de gestion des risques liés à l'IA qui tiennent compte des préjugés et des responsabilités potentiels, protégeant ainsi les intérêts des consommateurs et assurant la reddition de comptes à chaque étape.</li> </ul> <p><b>Exactitude des données, gouvernance et cybersécurité</b></p> <ul style="list-style-type: none"> <li>Accorder la priorité à l'accès à des données centralisées et de haute qualité tout en instaurant des mesures de gouvernance et de cybersécurité rigoureuses pour protéger les informations sensibles.</li> </ul> | <p><b>Collaboration et partenariats sectoriels</b></p> <ul style="list-style-type: none"> <li>Favoriser une collaboration proactive entre les organismes de réglementation, les fournisseurs de technologie et les assureurs afin d'échanger sur les pratiques exemplaires et de soutenir l'adoption sécuritaire des initiatives d'IA.</li> </ul> <p><b>Formation et surveillance humaine</b></p> <ul style="list-style-type: none"> <li>Donner aux courtiers la possibilité de suivre une formation continue tout en conservant une surveillance humaine active pour s'assurer que les résultats générés par l'IA sont compris de manière transparente et validés efficacement.</li> </ul> <p><b>Considérations relatives à l'impact environnemental et à la durabilité</b></p> <ul style="list-style-type: none"> <li>Intégrer la durabilité dans les stratégies d'IA en tenant compte de l'impact environnemental et de la consommation d'énergie des outils d'IA, en veillant à ce que les déploiements cadrent avec les objectifs ESG plus larges.</li> </ul> <p><b>Utilisation éthique et responsable de l'IA</b></p> <ul style="list-style-type: none"> <li>Cultiver une solide culture de littératie en IA fondée sur des principes éthiques en élaborant des lignes directrices claires qui préviennent les préjugés, favorisent l'équité et renforcent la confiance des consommateurs tout au long du cycle de vie de l'IA.</li> </ul> |





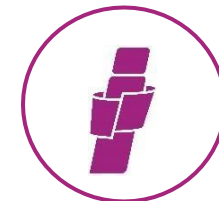
# Organisation de coopération et de développement économiques (OCDE) - Recommandation du Conseil sur l'IA

| Thèmes principaux   |   |
|---|---|
| <p><b>Croissance inclusive et développement durable</b></p> <ul style="list-style-type: none"> <li>• Promouvoir un écosystème de l'IA qui stimule la créativité humaine tout en réduisant les inégalités et en protégeant l'avenir de la planète.</li> <li>• Tirer parti des pratiques responsables de l'IA pour parvenir au développement durable et à la durabilité environnementale en mobilisant toutes les parties prenantes dès le début.</li> </ul> <p><b>Respect de l'état de droit et des droits de l'homme</b></p> <ul style="list-style-type: none"> <li>• Développer des solutions d'IA qui respectent rigoureusement les principes démocratiques en assurant la non-discrimination, une protection robuste des données et la protection de la liberté d'expression. Cette approche répond aux exigences réglementaires, en plus de prévenir la désinformation.</li> </ul> <p><b>Transparence et explicabilité</b></p> <ul style="list-style-type: none"> <li>• S'assurer que les systèmes d'IA sont conçus pour fournir des informations claires et contextuelles sur leurs sources de données sous-jacentes, leur logique et leurs processus décisionnels. Cela ouvre la « boîte noire » de l'IA, permettant aux consommateurs et aux parties prenantes de comprendre les capacités et les limites du système.</li> </ul> <p><b>Robustesse, sécurité et sûreté</b></p> <ul style="list-style-type: none"> <li>• Mettre en œuvre des protocoles techniques rigoureux et des mécanismes de protection qui préservent l'intégrité du système d'IA tout au long de son cycle de vie. Cela comprend la conception de systèmes qui peuvent être remplacés, réparés rapidement ou mis hors service en toute sécurité pour atténuer les préjudices potentiels ou les comportements non voulus.</li> </ul> | <p><b>Responsabilisation</b></p> <ul style="list-style-type: none"> <li>• Intégrer des processus de traçabilité et d'examen systématique tout au long du cycle de vie de l'IA pour s'assurer que tout parti pris, problème de confidentialité ou autre risque est rapidement identifié et géré.</li> <li>• La responsabilisation devrait être au cœur du cadre d'IA afin que tous les acteurs soient responsables du fonctionnement du système.</li> </ul> <p><b>Politiques nationales et coopération internationale pour une IA fiable</b></p> <ul style="list-style-type: none"> <li>• Encourager les gouvernements à investir dans la recherche sur l'IA et à faciliter le développement d'un écosystème inclusif et interopérable qui soutient l'innovation tout en respectant les normes éthiques. Il s'agit d'élaborer des politiques qui favorisent non seulement les progrès de l'IA au pays, mais aussi le dialogue et la collaboration à l'échelle internationale, ainsi que le renforcement des capacités humaines pour relever les défis futurs.</li> </ul> |



# Association Internationale des Contrôleurs d'Assurance (AICA) - Projet de document d'application sur la surveillance de l'IA

| Thèmes principaux  |   |
|--|---|
| <p><b>Gouvernance et responsabilité</b></p> <ul style="list-style-type: none"> <li>Tirer parti d'un cadre de gouvernance solide qui définit clairement les responsabilités et assure la surveillance tout au long du cycle de vie du système d'IA. Par exemple, « les assureurs doivent s'assurer de disposer d'un cadre de gouvernance robuste qui définit les responsabilités et assure une surveillance claire des systèmes d'IA tout au long de leur cycle de vie » et « le conseil d'administration doit posséder une expertise suffisante pour remettre en question efficacement la prise de décisions liées à la mise en œuvre de l'IA. » Ces mesures garantissent des résultats équitables pour les consommateurs et soutiennent la stabilité financière.</li> </ul> <p><b>Gestion des risques et proportionnalité</b></p> <ul style="list-style-type: none"> <li>Adopter une approche proportionnelle fondée sur le risque pour évaluer les systèmes d'IA en harmonisant les mesures de gestion des risques avec leur incidence potentielle sur les souscripteurs et la solidité financière globale.</li> </ul> <p><b>Robustesse, sûreté et sécurité</b></p> <ul style="list-style-type: none"> <li>Renforcer la fiabilité en mettant en œuvre des tests de rendement continus comme les « simulations de crise, l'analyse de sensibilité et les tests contradictoires » pour s'assurer que les systèmes d'IA fonctionnent avec intégrité dans toutes les conditions. En parallèle, appliquer des mesures de sécurité avancées qui « protègent les données et préviennent les cyberattaques », en particulier pour les systèmes qui prennent en charge des fonctions essentielles.</li> </ul> | <p><b>Transparence et explicabilité</b></p> <ul style="list-style-type: none"> <li>Développer des systèmes d'IA transparents et entièrement explicables en utilisant des outils comme SHAP ou LIME - en veillant à ce que les décisions soient « explicables et compréhensibles pour les consommateurs et les superviseurs ». Dans le même temps, intégrer l'équité dès la conception tout en instaurant des mécanismes de recours clairs afin que les parties touchées puissent facilement contester les décisions influencées par l'IA, respectant ainsi les droits fondamentaux et les normes éthiques.</li> </ul> <p><b>Équité, éthique et recours</b></p> <ul style="list-style-type: none"> <li>Établir une surveillance rigoureuse de la mise en œuvre de l'IA par des tiers en veillant à ce que les « contrats et les mesures de diligence raisonnable tiennent compte des risques et des limites opérationnels » inhérents aux systèmes externalisés. Conserver des enregistrements complets et traçables pour surveiller et auditer en permanence les déploiements de l'IA, garantissant ainsi une gouvernance solide tout au long du cycle de vie de l'IA.</li> </ul> |



# Association of British Insurers (ABI) - Guide sur l'IA : Idées pratiques pour commencer à utiliser l'IA responsable

## Thèmes principaux

### Principes de l'IA responsable

- Tirer parti d'une approche pratique qui « fournit une approche pratique pour l'application des cinq principes directeurs énoncés dans le document d'orientation sur l'IA du Royaume-Uni », y compris la sûreté, la sécurité et la robustesse, la transparence et l'explicabilité appropriées, l'équité, la responsabilité et la gouvernance, ainsi que la contestabilité et la réparation, pour s'assurer que tout développement de l'IA est ancré dans des principes éthiques et axés sur le consommateur.

### Cas d'utilisation de l'IA en assurance et en épargne à long terme

- Catégoriser et déployer systématiquement des cas d'utilisation de l'IA allant de la conception de produits (comme l'optimisation du portefeuille et la planification des soins aux personnes âgées) à la tarification et à la souscription (y compris la souscription prédictive et la tarification personnalisée), au traitement des demandes de règlement (comme la détection de la fraude et l'automatisation des demandes de règlement), en passant par le service à la clientèle ou la gestion des actifs pour stimuler l'innovation et l'efficacité opérationnelle.

### Gestion des risques liés à l'IA

- Surveiller les vulnérabilités des systèmes internes et les menaces externes, y compris les risques liés à la cybersécurité et à la dérive des modèles, et y répondre en posant des questions essentielles comme « Quel est le processus pour traiter les problèmes identifiés avec vos systèmes d'IA? » afin d'assurer une protection continue et la résilience des systèmes.

### Gouvernance des données et conformité à la réglementation

- Veiller à ce que la qualité des données soit robuste et à ce que l'utilisation des données demeure transparente, en respectant les cadres réglementaires établis, comme le règlement général sur la protection des données et la Loi sur la protection des données du Royaume-Uni.

### Considérations relatives au modèle d'IA

- Développer des modèles d'IA qui mettent l'accent sur l'explicabilité et la transparence, en intégrant des techniques comme LIME et SHAP pour « visualiser la boîte noire de l'apprentissage machine » tout en exigeant une revue humaine pour remettre en question les décisions automatisées, minimisant ainsi les préjugés et assurant des résultats équitables.

### Risques liés aux fournisseurs tiers

- Évaluer et gérer les risques associés aux fournisseurs tiers d'IA en mettant en œuvre des cadres rigoureux de surveillance contractuelle et de responsabilisation qui traitent de la sécurité des données, de la conformité et des répercussions opérationnelles connexes lors de la mobilisation de fournisseurs externes.

### Risques opérationnels, juridiques et liés à la cybersécurité

- Intégrer des systèmes de surveillance robustes, des plans de reprise après sinistre et des mesures de cybersécurité pour gérer les risques opérationnels et juridiques interconnectés, en veillant à ce que des questions telles que « Quels sont nos plans de reprise après sinistre et de continuité des activités? » soient traitées pour protéger l'ensemble de l'écosystème de l'IA.

### Collaboration et gouvernance

- Établir des lignes de responsabilité claires et une structure de gouvernance solide qui définit les rôles (à l'aide de modèles RACI) et favorise la transparence des communications entre les équipes techniques, les organismes de réglementation et les fonctions de surveillance interne afin d'assurer une surveillance humaine complète tout au long du cycle de vie de l'IA.

### IA responsable et digne de confiance

- Promouvoir l'IA responsable en déployant des systèmes dotés de mécanismes robustes de contestabilité et de recours qui permettent aux utilisateurs finaux de remettre en question les résultats générés par l'IA, intégrant ainsi l'intégrité éthique et la surveillance responsable à chaque étape de la conception et de la mise en œuvre de l'IA.

**Merci!**