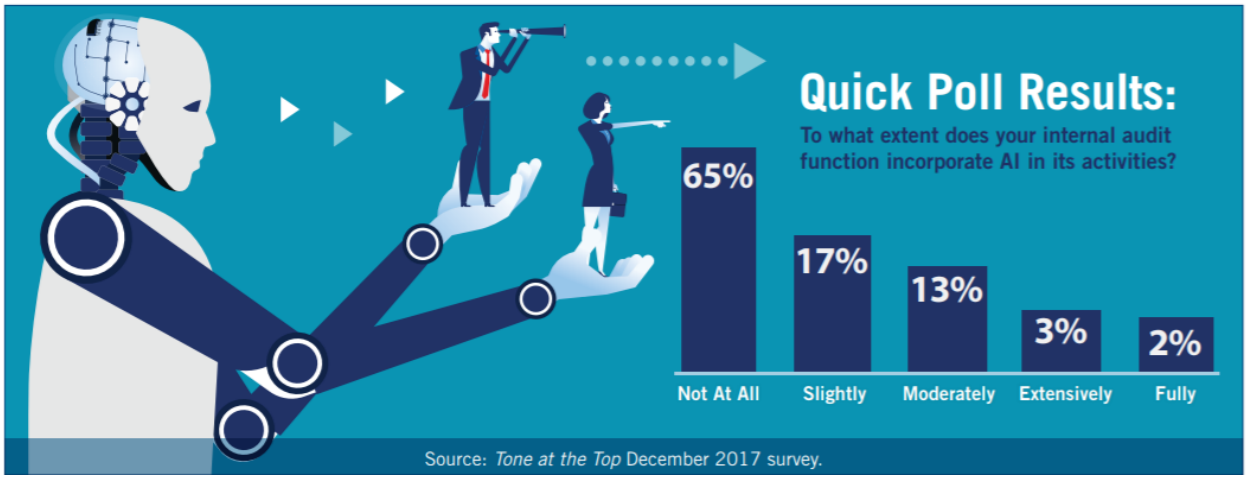
L'INTELLIGENCE ARTIFICIELLE (IA) ET L'AUDIT INTERNE



Intelligence artificielle : Où en sommes-nous?

Les entreprises sont aujourd'hui à l'aube de ce qui est la révolution technologique du 21e siècle, soit l'IA. Ce paradigme émergeant, qui commence à peine à transformer nos vies ainsi que nos organisations n'est pas une tendance éphémère à sous-estimer. L'impact sera énorme; en fait, du jamais vu!

Qu'est-ce que l'IA ?

On dit que l'IA est la dernière d'une série d'avancées rendues possibles grâce aux améliorations de la technologie (puissance augmentée, prix réduits). Nous constatons des avancées technologiques depuis des années mais avec l'IA, la capacité à traiter le « *Big Data* » change la donne de façon significative.

L'utilisation de l'IA touche tous les secteurs d'activité ainsi que toutes les industries. Elle a d'ailleurs permis de développer un certain nombre de nouvelles capacités et en automatiser d'autres.

Impacts organisationnels

Peu importe le secteur, la taille ou le type d'organisation, l'IA représentera un changement fondamental et significatif des façons de faire – autant à l'interne qu'auprès des parties prenantes externes.

Ce changement fondamental aura des répercussions jusqu'à maintenant impensables sur nos façons de faire. Ce que nous appelons communément l'« Industrie 4.0 » est arrivée et nous bousculera. De ce fait, nous devons nous y préparer et dès aujourd'hui.

Comment cela fonctionne?

L'IA permet aux machines de tirer enseignements de l'expérience vécue, d'intégrer des nouvelles données permettant d'apprendre en continue et de réaliser des tâches similaires à celles des humains. La plupart des exemples d'IA dont on entend parler aujourd'hui - des ordinateurs jouant aux échecs aux voitures autonomes - reposent largement sur l'apprentissage en profondeur (*deep learning*) et le traitement automatique du langage naturel (TALN).

Le TALN est une branche de l'IA qui aide les ordinateurs à comprendre, interpréter et manipuler le langage humain. Le TALN s'inspire de nombreuses disciplines, y compris l'informatique et la linguistique informatique, dans le but de combler l'écart entre la communication humaine et la capacité des systèmes informatiques à comprendre.

À l'aide de ces technologies, les ordinateurs peuvent être formés à la réalisation de tâches spécifiques en traitant de grandes quantités de données et en reconnaître des tendances dans les données.

Les algorithmes sont clés!

L'IA est alimentée par des algorithmes qui sont alimentés par le Big Data. Il est donc essentiel de maitriser le Big Data avant d'être capable d'implanter des processus d'IA et d'en tirer les bienfaits. L'étude de l'IIA intitulée « Perspectives internationales, Intelligence artificielle, Considérations pour la profession d'audit interne, Édition spéciale (2017) », définit le Big Data comme suit :

- Des grands volumes de données;
- Des volumes, variété, variabilité et vélocité de données si importantes que les organisations investissent dans des architectures de système, des outils et des pratiques spécifiquement conçus pour les gérer;
- Des données qui peuvent être générées par l'organisation, qu'elles soient publiques ou achetées.

Pour faire bon usage du Big Data, les organisations élaborent des algorithmes.

Les algorithmes définis

Un algorithme est une suite finie et non ambiguë d'opérations ou d'instructions permettant de résoudre un problème ou d'obtenir un résultat. C'est un ensemble de règles qu'un ordinateur doit suivre afin traiter rapidement de grandes quantités de données qu'un être humain ne peut raisonnablement pas traiter ou même comprendre.

Dans un article intitulé « *Understanding the four types of AI, from reactive robots to self-aware beings* » paru sur le site The Conversation, Arend Hintze, professeur adjoint en biologie intégrative et ingénierie informatique à l'Université d'État du Michigan, décrit quatre types d'IA :

Type I. Machine réactive : Les types les plus élémentaires de systèmes d'IA sont purement réactifs et ne permettent ni de constituer des mémoires, ni d'utiliser les expériences du passé pour alimenter les décisions futures. Les machines réactives répondent à une situation donnée toujours de la même manière.

Type II. Mémoire limitée : Les machines dotées d'IA à mémoire limitée peuvent regarder vers le passé mais ne peuvent pas créer des souvenirs ou « apprendre » d'expériences passées. Cette mémoire ne peut pas être créée en un instant, mais nécessite plutôt d'identifier des objets spécifiques et de les surveiller au fil du temps.

Type III. Théorie de l'esprit : Type III d'AI constitue le point entre les machines que nous avons et les machines que nous construirons à l'avenir. Les machines de cette classe, plus avancée, forment non seulement des points de vue du monde, mais également d'autres agents ou entités du monde. Ce type d'IA démontre une compréhension que les personnes, les créatures et les objets du monde peuvent avoir des pensées et des émotions qui affectent leur propre comportement.

Type IV. Conscience de soi : La dernière étape du développement de l'IA consiste à créer des systèmes pouvant former des représentations d'eux-mêmes. En fin de compte, nous, chercheurs en intelligence artificielle, devons non seulement comprendre la conscience, mais aussi construire des machines qui en sont dotées. Une telle machine serait consciente d'elle-même, connaîtrait son état et serait capable de prédire les sentiments des autres.

Ce que nous voyons aujourd'hui, pour la plupart, sont des manifestations de l'IA de Type I ou II. Les initiatives de recherche et développement en cours permettront aux organisations de progresser vers des applications pratiques de **Type III et IV**, ce qu'on appelle communément « la boîte noire »!

Opportunités pour les organisations

Les bienfaits que pourrait apporter l'IA pour toute organisation sont sans nul doute infinis. L'IA permettra aux entreprises d'accélérer et d'améliorer leurs processus et de réduire le risque d'erreur humaine. D'autre part, l'IA permettra de fournir des données à l'entreprise, grâce à ses activités, encore jamais exploitées du fait du volume de données émis.

Cette capacité d'analyse de données conférera également un avantage concurrentiel aux entreprises dans la mesure où l'IA permettra aux organisations, chacune individuellement et selon son investissement et engagement vis-à-vis l'IA, d'optimiser ses opérations et ses produits en exploitant davantage l'IA. Ceci

sera d'autant plus possible grâce l'apprentissage automatique (*machine learning*[1]) » associée à l'IA. Pour les entreprises utilisant l'IA :

- Le risque d'erreur est presque nul et une précision accrue est obtenue;
- Les machines intelligentes peuvent remplacer les êtres humains dans de nombreux domaines de travail; les robots peuvent effectuer certaines tâches laborieuses;
- La détection de fraudes dans les systèmes, basés sur des cartes à puce, est possible avec l'utilisation de l'IA;
- Les émotions qui interceptent souvent la pensée rationnelle d'un être humain ne constituent pas un obstacle pour les penseurs artificiels puisqu'ils sont dépourvus d'émotions, les robots peuvent raisonner logiquement et prendre les bonnes décisions car ils ne sont pas influencés par l'humeur qui affecte l'efficacité humaine;
- Des machines intelligentes peuvent être utilisées pour effectuer certaines tâches dangereuses;
- Le risque pour la santé et la sécurité des personnes est réduit lorsque l'IA est employée pour effectuer des tâches dangereuses,
- La capacité de faire de meilleures prévisions;
- La capacité de générer des revenus et d'accroître sa part de marché grâce aux initiatives.

Risques à considérer (*liste non-exhaustive*)

- Que la gouvernance encadrant l'utilisation de l'IA ne soit pas présente ou pas adéquate;
- Que des biais humains non identifiés soient intégrés dans la technologie de l'IA;
- Que des erreurs de logique humaine soient intégrées dans la technologie de l'IA;
- Que les tests et la surveillance de l'IA soient inadéquats aboutissent à des résultats éthiquement discutables;
- Que les produits et services d'IA provoquent préjudice, entraînant des problèmes financiers et / ou de réputation dommages;
- Que les clients ou d'autres parties prenantes n'acceptent ni n'adoptent les initiatives de l'organisation en matière d'IA;
- Résultats contestables dû à des tests ou une supervision inadéquate.

[1] *Machine learning* : est basé sur des approches statistiques pour permettre aux ordinateurs d'améliorer leurs performances à résoudre des tâches sans être explicitement programmés pour chacune et ce, à partir de données disponibles. Cette approche couvre la conception, l'évaluation, le développement et la mise en place de telles méthodes.

Ultimement, un des plus importants risques est que l'évolution de l'IA et, en l'occurrence l'apparition de la boîte noire, fait en sorte que les ordinateurs prennent le contrôle des êtres humains.

La fraude

Ce risque est omniprésent parmi les risques auxquels est soumise toute entreprise. L'IA, pour sa part repose sur des algorithmes développés par l'homme. Or, le biais humain (intentionnel ou non) peut affecter les données sur lesquelles reposent ces algorithmes, les conséquences pourraient alors être dévastatrices.

L'intention, la pression et la rationalisation sont autant de facteurs pouvant encourager un individu à commettre un acte de fraude. Ainsi, pour saisir la puissance et les impacts que pourraient avoir cette technologie et réduire les risques notamment des cyberattaques et des fraudes, il faudra avoir une compréhension stratégique et technique de comment est conçue l'IA et comment elle fonctionne.

Cette technologie, qui est à la pointe des avancées, nécessiterait une maitrise approfondie de l'environnement de contrôle.

Comment s'y préparer : les ressources indispensables à ce type de projet et le rôle de l'audit interne (AuI)

La réussite d'un projet de transformation numérique, et dans la situation de l'IA, des projets d'envergure significative va dépendre, en partie, des ressources qui seront responsables de développer lesdits projets. Cette même réussite dépendra également de la capacité d'une entreprise à évoluer à mesure où le projet avancera dans le temps, car, de nouveaux métiers ainsi que de nouvelles expertises verront le jour pendant le processus de création des projets de transformation en IA.

Il s'agit aujourd'hui pour les entreprises, de commencer à entrevoir les possibilités qui s'offriront à elles en matière d'emplois, car, comme le veut la théorie de la destruction créatrice initiée par Schumpeter en 1912, l'arrivée de cette nouvelle technologie fera disparaître beaucoup de métiers existants et en créera davantage. Le bouleversement sera tel, que si l'on en croit l'étude de l'*Institute For The Future and Dell Technologies* publiée en 2017, c'est plus de 85% des emplois que nous connaîtrons en 2030 qui n'existent pas encore aujourd'hui.

À cet instant, il semblerait plus qu'opportun de compter, comme ressources indispensable à un tel projet, des experts en gestion de projet, en technologies de l'information (TI), en IA, en AuI, en fraude ainsi qu'en éthique.

Quelles sont les menaces dont devraient se préoccuper les auditeurs internes?

En définitive, peu importe la manière dont elle sera utilisée pour gérer différentes opérations ou pour effectuer leur suivi, l'IA bouleversera sans aucun doute les façons de faire des auditeurs internes. Théoriquement, le recours à des intermédiaires agissant en tant « qu'agents de confiance », sera de moins en moins nécessaire puisque cette nouvelle technologie procurera une sécurité et une transparence de haut niveau.

Pourquoi l'IA doit être un sujet d'intérêt pour l'Audit interne ?

Les transformations organisationnelles sont monnaie courante de nos jours. Avec l'arrivée de l'IA, cette tendance se verra amplifiée et les transformations organisationnelles plus importantes et coûteuses. Dans un contexte de projets importants avec risques de pertes significatives, les AuI comme experts en identification des risques et des moyens à les gérer, sont parfaitement placés pour jouer un rôle crucial dans cette nouvelle ère!

Par contre, pour être pertinent dans notre nouveau monde, le profil de l'AuI va devoir changer autant d'un point de vue formation que dans sa capacité d'évaluer les risques des situations émergentes. La fonction d'AuI (FAI) peut, plus que jamais, être précurseur en tant que facilitateur de l'IA pour son organisation mais seulement s'il s'adapte et ce dès maintenant. Si l'AuI agit maintenant, il pourra continuer à démontrer qu'il est créateur de valeur ajoutée et non uniquement une fonction de contrôle. L'AuI :

- Pourra assister son organisation à identifier les opportunités d'intégration de l'IA dans ses façons de faire;
- Pourra continuer à jouer le rôle historique d'identification de risques, de moyens de gestion de ces derniers, de spécialiste en processus d'affaires;
- Devra adapter ses procédés d'audit;
- Sera composé de ressources ayant des profils différents.

Comme partenaire d'affaires, l'AuI pourra jouer un rôle clé lors des phases de planification, d'implantation et d'optimisation des processus d'affaires organisationnels.

Pour se préparer, les auditeurs internes doivent comprendre les bases de l'IA, les rôles que l'AuI devrait jouer ainsi que les risques et les opportunités que représente l'IA. L'AuI devrait tirer profit du Cadre de référence de l'IIA, voir ci-dessous, pour fournir des méthodes systématiques et rigoureuses visant à évaluer et à améliorer l'efficacité des processus de gestion des risques, de contrôle et de gouvernance liés à l'IA.

L'AuI devra :

- Savoir comment fonctionne l'IA;
- Comprendre les risques et les opportunités que l'IA représente;
- Déterminer si les résultats de l'IA correspondent aux attentes;
- Être capables de recommander ou de prendre des mesures correctives le cas échéant.

(Source : https://global.theiia.org/translations/PublicDocuments/GPI-Artificial-Intelligence-Part-II-French.pdf)

De telles compétences seront requises au niveau des trois lignes de défense. La direction générale et le Conseil d'administration devront également connaître le fonctionnement de l'IA et comprendre les risques et opportunités qu'elle représente. L'AuI peut aider une organisation à évaluer, comprendre et communiquer la mesure dans laquelle l'IA aura un effet (négatif ou positif) sur la capacité de cette organisation à créer de la valeur à court, moyen, ou à long terme.

L'AuI :

- Comprend les objectifs stratégiques de l'organisation et les processus mis en œuvre pour atteindre ces objectifs;
- Est en mesure d'évaluer si les activités d'IA contribuent à la réalisation de leurs objectifs;
- Peut fournir une assurance interne sur les activités de management des risques de la direction générale pertinentes au regard des risques de l'IA;
- Est perçu comme un conseiller de confiance pouvant soutenir l'adoption de l'IA pour améliorer les processus de l'organisation ou l'offre de produits et de services.

Actions à entreprendre par l'AuI :

- Inclure l'IA dans son évaluation des risques et envisager la possibilité de l'inclure également dans son plan d'audit fondé sur une approche par les risques;
- Participer activement aux projets d'IA dès leur début, en fournissant des conseils et des points de vue qui contribuent à la réussite de leur mise en œuvre;

- Fournir une assurance sur la gestion des risques liés à la fiabilité des algorithmes sous-jacents et des données sur lesquelles reposent les algorithmes;
- S'assurer que les questions éthiques et morales qui peuvent entourer l'utilisation de l'IA par l'organisation sont traitées;
- Donner, comme pour toute autre initiative importante, une assurance sur les structures de gouvernance.

Évidemment, l'AuI ne devrait pas être chargé, ni être responsable, de la mise en œuvre des processus, politiques ou procédures d'IA afin d'éviter toute atteinte perçue ou réelle à son indépendance et à son objectivité.

L'AuI devrait aborder l'IA comme il traite les autres domaines, c'est-à-dire avec une approche systématique et méthodique afin d'évaluer et d'améliorer l'efficacité des processus de management des risques, de contrôle et de gouvernance liés à l'IA.

Revaloriser la cyber-résilience

Selon le rapport de l'IIA, *Perspectives internationales, Intelligence artificielle, Considérations pour la profession d'audit interne*, Édition spéciale (2017), les menaces sur la cybersécurité sont plus que jamais présentes. L'adoption et l'évolution de l'IA obligeront les organisations à revaloriser leurs capacités en matière de cyber-résilience, approche maintenant adoptée par les organisations[2]. Avec l'IA, les décisions seront progressivement confiées à des algorithmes inédits, complexes et opaques, qui utilisent des données très volumineuses. Il sera donc crucial de protéger ces systèmes contre des forces externes et malveillantes. La cyber-résilience est essentielle pour toute organisation qui dépend de plus en plus de l'IA.

Aussi complexe que soit la cybersécurité, selon l'étude, il existe quatre domaines clés où l'AuI peut avoir un effet immédiat, notamment en :

- Fournissant une assurance sur le degré de préparation et la réponse de l'organisation aux cyber-menaces;
- Communiquant à la direction générale et au Conseil le niveau de risque encouru par l'organisation et les efforts déployés pour faire face à ces risques;
- Travaillant en partenariat avec les TI et d'autres parties pour s'assurer que des réponses et des défenses efficaces sont en place;

[2] The Cyber Resilience Blueprint: A New Perspective on Security
https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf

- Facilitant la communication et la coordination entre toutes les parties de l'organisation en matière de risques.

Les effets potentiellement désastreux d'une faille de cybersécurité concernant l'intelligence artificielle sont à gérer par la mise en place de mesures de cybersécurité au sein des équipes d'AuI.

Régulateurs

A ce jour, il n'existe aucune réglementation dédiée exclusivement à l'IA. Toutefois, certaines parties de réglementations existantes peuvent être pertinentes pour les activités d'IA. Les régulateurs et les organismes de normalisation du monde entier ont fait part de leurs inquiétudes au travers des recherches conduites, de documents de réflexion, de recommandations et de lignes directrices. Le Cadre de référence IIA pour l'audit de l'IA peut lui faciliter la tâche.

Par ailleurs, un document intitulé « Déclaration de Montréal pour un développement responsable de l'IA » a été élaboré par l'Université de Montréal et plusieurs sommités en la matière de la communauté montréalaise, notamment Yoshua Bengio, et qui énonce des principes éthiques de l'utilisation de l'IA (https://www.declarationmontreal-iaresponsable.com/la-declaration).

Création d'un sous-comité du Conseil d'administration?

Nous pensons qu'il serait opportun de considérer la création d'un sous-comité du Conseil dédié au bon fonctionnement de l'IA. Ce comité pourrait avoir comme mission de s'assurer de la bonne utilisation de l'IA en exerçant ses fonctions de manière objective et indépendante. Ce sous-comité devrait être composé d'au-moins un expert dans les domaines suivants : AuI, gestion de crise, fraude, éthique, technologie de l'information, cybersécurité / cyber-résilience.

Comment les auditeurs internes doivent-ils se préparer : les certifications à valeur ajoutée

En plus des compétences dont devraient jouir les AuI, une liste non exhaustive des certifications qui pourraient mieux outiller les AuI à l'IA :

- CIA : Auditeur interne certifié ;
- CRMA : Auditeur certifié en assurance sur la maîtrise de la gestion du risque ;
- CISA : Auditeur certifié en système d'information ;
- CFE : Examinateur de fraude certifié.

La profession d'auditeur interne est plus que sujette à la robotisation et à l'automatisation de ses tâches. C'est pourquoi il nous faut acquérir une compréhension pleine de ce qu'est réellement l'IA, ainsi qu'une expertise sur les risques qui l'entoure. Plus que jamais, les auditeurs internes devront s'adapter et acquérir les connaissances nécessaires pour gérer l'environnement de contrôle de l'IA.

En plus des compétences techniques et des expériences antérieures, les auditeurs internes doivent être prêts à explorer de nouveaux horizons en termes de transformations et robotisation. Pour ce faire, ces derniers doivent faire preuve de sens d'analyse, de capacité d'intégration, de volonté et d'appétence pour l'apprentissage.

En plus des certifications à valeur ajoutée pour une telle expertise, les auditeurs internes devront se montrer proactif et s'éduquer eux-mêmes sur l'IA. Pour autant, il y a fort à parier que le « tone at the top » jouera un rôle important quant à l'éducation des auditeurs internes sur l'IA. Il s'agit donc pour les directions d'embarquer toutes les parties prenantes nécessaires avec eux pour leurs projets de transformations.

En effet, quand un auditeur effectuera un échantillon pour tester un contrôle, l'IA analysera la population totale, reflétant ainsi la situation réelle de cette population.

Conclusion

Le Cadre de référence IIA pour l'audit de l'IA permettra aux auditeurs internes d'aborder les services de conseil et d'assurance relatifs à l'IA, de manière systématique et disciplinée. Que les technologies et activités d'IA de l'organisation soient développées en interne, par le biais d'outils comme AutoML ou par un tiers, l'AuI devrait être préparé à épauler le Conseil et la direction générale, à se coordonner avec la première et la deuxième ligne de défense et à fournir une assurance sur les dispositifs de management des risques, de gouvernance et de contrôle associés à l'IA.

Prochain sujet – État de question #2

Bien comprendre l'utilisation de l'IA dans les organisations pour bien intervenir

L'état de question #1 produit par : Pierre Taillefer, associé BDO, Florian Bodart, Consultant – Services-conseils en risque BDO et Pascal Théoret, directeur Bureau de la vérification interne, Université de Montréal

Références

https://www.declarationmontreal-iaresponsable.com/la-declaration

Perspectives internationales, Intelligence artificielle, Considérations pour la profession d'audit interne, Édition spéciale (2017) :

https://global.theiia.org/translations/PublicDocuments/GPI-Artificial-Intelligence-Part-I-French.pdf

https://global.theiia.org/translations/PublicDocuments/GPI-Artificial-Intelligence-Part-II-French.pdf

https://na.theiia.org/periodicals/Public%20Documents/GPI-Artificial-Intelligence-Part-III.pdf

https://global.theiia.org/translations/PublicDocuments/GPI-Agility-and-Innovation-FRENCH.pdf

https://docs.ifaci.com/wp-content/uploads/2018/03/tone-at-the-top-85-ia.pdf

https://mag.ifaci.com/les-metiers-de-laudit-et-du-controle-internes-vont-se-reinventer-avec-lintelligence-artificielle/

http://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616

http://www.iftf.org/future-now/article-detail/realizing-2030-dell-technologies-research-explores-the-next-era-of-human-machine-partnerships/

The Cyber Resilience Blueprint: A New Perspective on Security :
https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf