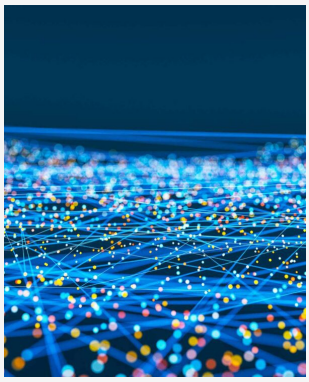
OSLER

Le rôle de la norme ISO/IEC 42001 dans la gouvernance de l'intelligence artificielle

17 JUILLET 2024 11 MIN DE LECTURE



Expertises Connexes

- Gestion de risques et réponse aux crises
- Gouvernance d'entreprise
- Intelligence artificielle
- Opérations commerciales en matière de technologie
- Respect de la vie privée et gestion de l'information
- Technologie

Auteurs(trice): Sam Ip, Joseph Ierullo, Iman Jaffari

Aperçu mondial des normes émergentes en matière d'intelligence artificielle

Les progrès rapides de l'intelligence artificielle (IA) ont créé un paysage complexe de défis réglementaires et de considérations éthiques. Pour s'y retrouver, plusieurs cadres et normes réglementaires clés ont été élaborés.

Au Canada, la Loi proposée sur l'intelligence artificielle et les données (partie 3 du projet de loi C-27) vise à réglementer de façon exhaustive les systèmes d'IA, en mettant l'accent sur la protection des personnes et la réglementation du développement et de l'adoption responsables de l'IA. Dans l'Union européenne (UE), la *loi sur l'intelligence artificielle* a été finalisée et approuvée par le Conseil de l'UE le 21 mai 2024. Cette loi adopte une approche réglementaire fondée sur le risque, en classant les systèmes d'IA par niveau de risque et en imposant des exigences réglementaires correspondantes. Parallèlement, l'AI Risk Management Framework (cadre de gestion des risques liés à l'intelligence artificielle) du National Institute of Standards and Technology des États-Unis offre aux organisations des lignes directrices qui leur permet d'évaluer et d'atténuer les risques liés à l'IA. En plus de ces cadres, le secteur de l'IA regorge de projets de lois, de principes, de lignes directrices et de codes de conduite. Cette mosaïque d'instruments souligne la nécessité et le rôle des normes internationales pour assurer l'uniformité et la cohérence en ce qui concerne l'utilisation, l'adoption et la gouvernance de l'IA.

Aperçu de la norme ISO/IEC 42001 : système de management de l'intelligence artificielle

Au milieu de ces divers développements, l'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) ont créé la norme ISO/IEC 42001 grâce à l'effort collaboratif d'un groupe diversifié d'intervenants du secteur de l'IA, la première norme mondiale et unifiée des systèmes de management pour l'IA. Publiée récemment en décembre 2023, cette norme internationale fournit aux organisations un cadre complet et certifiable pour l'établissement, la mise en œuvre et l'amélioration continue d'un système de management de l'IA. La norme ISO/IEC 42001 met l'accent sur l'éthique, la

transparence, la responsabilisation, l'atténuation des biais, la sécurité et le respect de la vie privée en couvrant les éléments essentiels du développement et du déploiement de l'IA.

La norme ISO/IEC 42001 n'existe pas isolément. Elle fait partie d'un ensemble plus vaste de normes liées à l'intelligence artificielle élaborées par l'ISO et la CEI, notamment les normes suivantes :

- ISO/IEC 22989 : établit des définitions en langage commun de la terminologie de l'IA et décrit les concepts émergents dans ce domaine
- ISO/IEC 23053 : établit un cadre pour la description d'un système d'IA générique utilisant la technologie de l'apprentissage machine, favorisant l'interopérabilité entre les systèmes d'IA et leurs composants
- ISO/IEC 23894 : établit des lignes directrices pour la gestion des risques liés à l'IA dans les organisations qui développent et déploient des produits et services d'IA, décrit les processus d'intégration des stratégies de gestion des risques liés à l'IA dans les activités organisationnelles et aide à cerner, à évaluer et à atténuer efficacement ces risques.

Portée et application

Bien que ces normes traitent d'aspects et d'applications particuliers de l'IA, la norme ISO/IEC 42001 se distingue comme une norme complète de système de management qui offre une approche pratique de la gestion des risques et des occasions liés à l'IA dans l'ensemble d'une organisation. En adoptant cette norme et son approche globale des diverses applications d'IA, les organisations peuvent promouvoir une utilisation responsable de l'IA, renforcer la confiance dans leurs applications d'IA et assurer la conformité aux normes juridiques et réglementaires. Non seulement ce cadre favorise la responsabilisation, mais il encourage aussi l'innovation au sein d'une structure bien définie.

De plus, la norme ISO/IEC 42001 est conçue pour les organisations de toutes tailles qui développent, fournissent et utilisent des produits ou des services fondés sur l'intelligence artificielle dans divers secteurs d'activité. Cette norme s'applique aux entités des secteurs privé et public, y compris les entreprises, les organismes sans but lucratif et les organismes gouvernementaux, et couvre tout le cycle de vie des systèmes d'IA, depuis leur développement jusqu'à leur déploiement.

Concepts clés de la norme ISO/IEC 42001

Les concepts clés qui constituent le fondement d'un système de management efficace de l'IA selon la norme ISO/IEC 42001sont les suivants :

- Contexte organisationnel : les organisations doivent bien comprendre leur environnement interne et externe lorsqu'elles déterminent les besoins et les attentes des intervenants, comme les clients, les organismes de réglementation et les employés. Identifier ces contextes permet aux organisations d'ajuster leurs systèmes d'IA pour qu'ils soient pertinents et efficaces, en tenant compte des capacités internes et en répondant aux demandes externes.
- Engagement de la direction : la haute direction doit établir des politiques claires en matière d'IA, définir les rôles et les responsabilités et intégrer la gouvernance de l'IA dans ses objectifs stratégiques globaux. Cette approche descendante assure le soutien et la

priorisation des initiatives et des projets d'IA.

- Planification des systèmes de management de l'IA : les organisations doivent adopter une approche proactive de la gestion des systèmes d'IA en déterminant les risques et les occasions dès le début. Il s'agit notamment de collaborer avec divers intervenants afin d'élaborer des plans exhaustifs pour les objectifs de l'IA, des stratégies de gestion des risques et des méthodes permettant de tirer parti des occasions liées à l'IA au sein de l'organisation.
- Affectation des ressources : un soutien adéquat aux systèmes d'IA est essentiel à leur gestion et à leur mise en œuvre efficaces. Pour ce faire, les organisations doivent affecter suffisamment de ressources financières, technologiques et humaines pour maintenir et améliorer les compétences en exploitation de l'IA. À titre d'exemple, mentionnons la budgétisation des outils de gouvernance de l'IA, l'embauche de spécialistes de l'éthique de l'IA et la formation continue sur les systèmes d'IA internes.
- Contrôles opérationnels : Il est essentiel de mettre en œuvre des processus responsables de développement, de déploiement et d'utilisation de l'IA tout au long du cycle de vie, notamment en collaborant avec les intervenants concernés pour établir des protocoles précis et détaillés afin d'assurer la sécurité, le respect de la vie privée et l'équité des opérations d'IA dans l'ensemble de l'organisation.
- Suivi du rendement : la création de mécanismes d'évaluation continue pour évaluer le rendement de l'IA et repérer les points à améliorer est essentielle pour assurer la précision et la conformité. Il peut s'agir d'audits périodiques ou de vérifications ponctuelles visant à s'assurer du respect des mesures, des objectifs organisationnels et des normes réglementaires clairement définis.
- Amélioration continue : Pour compléter le processus de gestion global, il est essentiel d'établir des étapes de mise à jour et d'amélioration des systèmes d'IA en fonction des évaluations du rendement, des technologies émergentes et de l'évolution des exigences réglementaires. Il s'agit de favoriser l'amélioration continue en intégrant des commentaires précis, en affinant les pratiques de gouvernance de l'IA et en s'assurant que le système de management de l'IA demeure aligné sur les objectifs organisationnels et conforme aux règlements applicables.

La norme ISO/IEC 42001 comporte également quatre annexes qui offrent des conseils supplémentaires et complémentaires :

- Annexe A [Objectifs des contrôles de référence] fournit des lignes directrices détaillées pour la construction de systèmes d'IA, y compris des étapes précises pour leur conception, leur développement et leur mise à l'essai. Cette annexe définit des objectifs et des contrôles de référence, couvrant des domaines tels que la provenance des données, la gestion de la qualité du système, la sélection du modèle et l'évaluation du rendement.
- Annexe B [Directives de mise en œuvre des contrôles] offre des conseils précis sur la mise en œuvre des contrôles, qui détaillent les mesures d'atténuation des risques, la gouvernance des données et les pratiques éthiques en matière d'IA. Cette annexe comprend des exemples pratiques et des listes de contrôle pour chaque domaine de contrôle énuméré, ce qui aide les organisations à assurer une couverture complète des

exigences en matière de gestion de l'IA.

- Annexe C [Objectifs de l'IA et sources de risque] fournit un cadre permettant aux organisations de gérer les complexités de la mise en œuvre des systèmes de management de l'IA. Cette annexe met l'accent sur des objectifs clés comme l'équité, la sécurité, la sûreté et le respect de la vie privée tout en détaillant les risques potentiels, comme les risques de biais, d'empoisonnement des données, les problèmes de fiabilité du réseau et les écarts de rendement.
- Annexe D [Normes pour des domaines et secteurs d'activité précis] fournit des directives générales sur l'application de la norme dans des secteurs particuliers comme les soins de santé, les services financiers et la défense. Cette annexe souligne également l'importance d'intégrer les pratiques de gestion de l'IA à d'autres normes sectorielles afin d'améliorer la conformité et l'efficacité dans divers contextes opérationnels.

Répercussions

L'adoption de la norme ISO/IEC 42001 aide non seulement les organisations à s'assurer que leurs systèmes d'IA sont développés et gérés de façon responsable, mais elle renforce également leur fiabilité. De nombreuses organisations connaissent déjà la norme ISO/IEC 27001, la norme internationale pour les systèmes de management de la sécurité de l'information. Cette norme met l'accent sur la gestion du risque, l'amélioration continue et l'engagement organisationnel à l'égard de la sécurité et de l'éthique. La norme ISO/IEC 42001 complète la norme ISO/IEC 27001 en proposant une approche globale de l'atténuation des risques liés à la sécurité de l'information. Elle répond aux difficultés propres à l'IA, comme la confidentialité dans l'entraînement des modèles et le respect de la vie privée, les problèmes d'intégrité comme les biais et la falsification, et s'assure de la disponibilité des processus essentiels de l'IA nécessaires à une utilisation autorisée. Cette intégration permet aux organisations d'établir des politiques cohésives qui maintiennent la cohérence et gèrent efficacement les risques liés à l'IA dans leurs systèmes existants de management de la sécurité de l'information. La certification et les audits par rapport à des normes mondialement reconnues, comme la norme ISO/IEC 27001, peuvent renforcer la confiance des intervenants dans les capacités d'IA d'une organisation et lui permettre de se démarquer de la concurrence sur le marché.

Les premières étapes consistent à se familiariser avec les exigences et les lignes directrices de la norme ISO/IEC 42001, à évaluer les pratiques actuelles en matière d'IA afin de repérer les lacunes et à élaborer un plan complet de mise en œuvre. Faire appel à des experts-conseils spécialisés dans les normes ISO/IEC 42001 et ISO/IEC 27001 peut apporter une aide précieuse pendant le processus. Cette expertise conjointe peut simplifier le processus d'évaluation des risques et de création de politiques en intégrant des éléments d'utilisation éthique de l'IA, de transparence et de confidentialité des données. Une évaluation des écarts peut révéler les changements nécessaires dans les rôles organisationnels précisés dans la norme, qui imposent des responsabilités de gouvernance de l'IA. Elle met également en lumière les mises à jour à apporter aux programmes de sensibilisation à la sécurité et les investissements à faire dans les technologies prenant en charge l'IA et les systèmes de management de la sécurité de l'information.

Pour la suite

Bien que la LIAD fasse actuellement l'objet d'une étude article par article par un comité parlementaire, son adoption éventuelle obligerait les organisations à établir un cadre de responsabilisation pour le déploiement et l'adoption de l'IA. Il convient de noter que des normes certifiables comme la norme ISO/IEC 42001 pourraient jouer un rôle crucial, en

particulier pour les organisations exerçant leurs activités ou faisant des affaires dans plusieurs territoires, en fournissant un cadre pour l'établissement et le maintien d'un système d'IA d'importance internationale.