Revue-IRS

Revue Internationale de la Recherche Scientifique (Revue-IRS)

ISSN: 2958-8413

Vol. 3, No. 3, Mai 2025

L'Impact de l'Intelligence Artificielle sur le Contrôle Interne et la Gestion des Risques

MAAROUFI Abdelkader, BRABIJE Hanane

Laboratoire d'Économie Sociale, Solidaire et Développement Local.

Faculté Mohammed Premier , Oujda. Maroc

Abstract: L'intelligence artificielle (IA) s'impose progressivement comme un levier stratégique dans la modernisation du contrôle interne et la gestion des risques organisationnels. En réponse à la complexité croissante des environnements économiques et réglementaires, elle offre des outils puissants d'analyse prédictive et de traitement des données en temps réel. Cette étude interroge la capacité de l'IA à transformer durablement les systèmes de contrôle interne, historiquement fondés sur des approches réactives et standardisées, en dispositifs proactifs et intelligents. Néanmoins, son intégration soulève des préoccupations majeures en matière de biais algorithmiques, de transparence des modèles et de gouvernance éthique. À travers une revue critique de la littérature et l'analyse de cas concrets, notamment dans le contexte marocain, cette recherche identifie les conditions nécessaires à une adoption responsable et efficace de l'IA dans les processus de contrôle interne, en cohérence avec les référentiels internationaux tels que le COSO ou l'ISO.

Keywords: Intelligence artificielle (IA), Gestion des risques, Contrôle interne, Gouvernance éthique.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**15575377**

1 Introduction

La transformation numérique bouleverse profondément les modes de fonctionnement des organisations, dans un contexte marqué par une complexité croissante des environnements économiques, réglementaires et technologiques. Les entreprises doivent aujourd'hui composer avec une multiplicité de risques : cyberattaques, fraudes financières, erreurs de reporting, ou encore non-conformité réglementaire (Deloitte, 2023). À cette dynamique s'ajoute une exigence renforcée de transparence, de traçabilité et de performance. Ces défis, amplifiés par la mondialisation et la digitalisation, mettent à l'épreuve les systèmes traditionnels de contrôle interne et de gestion des risques, souvent jugés trop rigides ou réactifs (COSO, 2017).

Dans ce contexte, l'intelligence artificielle (IA) s'impose comme une technologie stratégique, porteuse d'opportunités majeures. Par sa capacité à traiter d'importants volumes de données en temps réel, à détecter des anomalies et à anticiper des tendances, l'IA promet d'améliorer significativement l'efficacité du contrôle interne et des dispositifs de maîtrise des risques (Accenture, 2022). Pourtant, cette intégration ne va pas sans poser question. L'automatisation des processus, la faible explicabilité de certains algorithmes (phénomène de "boîte noire"), ou encore les biais décisionnels induits par les données d'entraînement, interrogent sur les limites, les risques et les implications éthiques de ces technologies (Binns, 2020) (Russell & Norvig, 2020).

Dès lors, une question centrale se pose : **dans quelle mesure l'intelligence artificielle peut-elle transformer durablement les pratiques de contrôle interne et de gestion des risques, tout en garantissant une gouvernance à la fois efficace et éthique ?** Ce questionnement est d'autant plus pertinent qu'il s'inscrit dans un moment charnière où les organisations doivent adapter leurs cadres de référence, comme ceux proposés par le **COSO** ou la norme **ISO 31000**, aux nouvelles réalités imposées par l'IA (ISO, 2018).

Pour éclairer cette problématique, cette communication adopte une approche méthodologique en quatre temps. Elle repose d'abord sur une **revue critique de la littérature académique** portant sur les interactions entre IA, contrôle interne et gestion des risques. Elle s'appuie ensuite sur **des études de cas sectorielles**, notamment dans les secteurs bancaire, public et technologique, afin d'illustrer concrètement les bénéfices et les défis observés sur le terrain. Enfin, elle mobilise un **cadre conceptuel structuré** autour du référentiel COSO et des normes ISO pour proposer une analyse approfondie et contextualisée.

L'objectif de ce travail est triple :

1. Identifier les **apports concrets** de l'IA dans les processus de gouvernance interne ;
2. Mettre en lumière les **limites techniques, organisationnelles et éthiques** de son utilisation ;
3. Formuler des **recommandations pratiques** pour favoriser une intégration efficace, transparente et responsable de ces technologies dans les dispositifs de contrôle interne.

2 Cadres théoriques et concepts fondamentaux

2.1 Le contrôle interne selon le COSO

Le cadre COSO (Committee of Sponsoring Organizations of the Treadway Commission) constitue une référence majeure en matière de contrôle interne. Il vise à fournir une assurance raisonnable quant à la réalisation des objectifs stratégiques, à la fiabilité de l'information financière, et à la conformité réglementaire (COSO, 2013). Il repose sur cinq composantes clés:

1. L'environnement de contrôle
2. L'évaluation des risques
3. Les activités de contrôle
4. L'information et la communication
5. Le pilotage et la surveillance

Le COSO a été actualisé en 2013, puis enrichi dans le cadre de son modèle d'Enterprise Risk Management (ERM) en 2017, afin de mieux intégrer la gestion des risques stratégiques et la gouvernance d'entreprise (COSO, 2017).

2.2 Principes de la gestion des risques selon ISO 31000

La norme ISO 31000, quant à elle, propose un cadre de gestion des risques applicable à tout type d'organisation. Elle repose sur trois piliers :

- Les **principes de la gestion des risques**, tels que la création de valeur, l'intégration dans la culture organisationnelle, et la prise de décision éclairée.
- Un **cadre de gouvernance**, incluant les rôles et responsabilités.
- Un **processus structuré**, allant de l'identification à l'évaluation, en passant par le traitement et le suivi des risques (ISO, 2018).

L'approche ISO est davantage orientée vers une gestion proactive des incertitudes, complétant utilement le cadre COSO par son aspect normatif et transversal.

2.3 Fondamentaux de l'intelligence artificielle

L'intelligence artificielle (IA) regroupe un ensemble de techniques permettant aux systèmes informatiques d'exécuter des tâches qui requièrent normalement l'intelligence humaine, telles que l'apprentissage, le raisonnement, la reconnaissance d'images ou la compréhension du langage (Russell & Norvig, 2020).
Les principaux sous-domaines incluent :

- Le **machine learning**, qui permet aux algorithmes d'apprendre à partir des données.
- Le **deep learning**, sous-domaine du machine learning basé sur les réseaux de neurones profonds.
- Le **traitement automatique du langage naturel (NLP)**, qui permet à la machine d'analyser et de comprendre le langage humain (Goodfellow et al., 2016).

Toutefois, ces technologies présentent des limites. L'explicabilité des modèles (XAI – explainable AI) est un enjeu central, en particulier dans les environnements réglementés comme l'audit ou le contrôle interne, où la "boîte noire" algorithmique pose des défis majeurs en matière de transparence (Gunning & Aha, 2019).

3 L'apport de l'intelligence artificielle dans la gestion des risques et le contrôle interne

L'intelligence artificielle transforme les pratiques organisationnelles en permettant une approche proactive et automatisée du contrôle interne et de la gestion des risques. Plusieurs apports sont à souligner dans cette dynamique.

3.1 Automatisation des processus et gains d'efficacité

L'un des principaux avantages de l'IA réside dans l'automatisation des tâches complexes et répétitives. Dans le domaine du contrôle interne, des algorithmes peuvent analyser en temps réel des milliers de transactions financières afin de détecter des anomalies ou des schémas frauduleux (KPMG, 2021). Des outils d'automatisation, tels que les robots logiciels (RPA – Robotic Process Automation) combinés à l'IA, permettent d'alléger la charge de travail des auditeurs internes tout en augmentant la précision des contrôles (Deloitte, 2022).

3.2 Détection d'anomalies et analyse prédictive

L'analyse prédictive, alimentée par le machine learning, permet d'anticiper des défaillances potentielles ou des irrégularités en s'appuyant sur des historiques de données. L'IA est ainsi capable de repérer des signaux faibles invisibles pour les approches traditionnelles, améliorant la réactivité des dispositifs de gestion des risques (PWC, 2020). Par exemple, dans l'audit interne, certaines firmes utilisent des modèles prédictifs pour cibler les zones à risque élevé dans les plans d'audit (IBM Institute for Business Value, 2021) .

3.3 Meilleure identification des risques émergents

Les technologies d'IA offrent également la possibilité de capter des risques émergents par le croisement de données structurées (comptabilité, rapports) et non structurées (emails, commentaires, réseaux sociaux). Le traitement automatique du langage naturel (NLP) joue un rôle clé dans cette capacité à intégrer des sources hétérogènes pour une surveillance dynamique des risques (Campolo et al., 2017).

3.4 Amélioration continue des dispositifs de contrôle

Enfin, l'IA permet une boucle d'amélioration continue dans les processus de contrôle interne. Les systèmes apprennent des incidents passés pour affiner leurs prédictions et adapter les seuils d'alerte. Cette évolution vers des systèmes intelligents favorise une gouvernance adaptative, plus résiliente face aux changements environnementaux (EY, 2021).

4 Limites et risques liés à l'intelligence artificielle

Si l'IA représente une avancée majeure pour le contrôle interne et la gestion des risques, son intégration soulève de nombreuses préoccupations, tant sur le plan technique qu'éthique. Ces limites doivent être rigoureusement analysées pour garantir une utilisation responsable et durable.

4.1 Biais algorithmiques et discrimination

Les algorithmes d'IA sont fortement dépendants des données sur lesquelles ils sont entraînés. Lorsque ces données reflètent des biais historiques ou culturels, les modèles reproduisent et amplifient ces inégalités. Dans le domaine du crédit, par exemple, des systèmes de scoring automatisé ont discriminé certaines populations minoritaires (Barocas & Selbst, 2016). Ces biais peuvent avoir des conséquences juridiques, réglementaires et réputationnelles importantes (Eubanks, 2018).

4.2 Opacité des modèles et "boîte noire"

De nombreux modèles de machine learning, notamment les réseaux de neurones profonds, sont peu explicables pour les utilisateurs finaux. Cette opacité limite leur auditabilité et rend difficile la compréhension des décisions prises par l'algorithme (Burrell, 2016). Dans un contexte de contrôle interne, cette absence de transparence peut compromettre la confiance des parties prenantes et empêcher une validation réglementaire (Doshi-Velez & Kim, 2017).

4.3 Risques de cybersécurité

L'introduction de l'IA accroît la surface d'exposition aux cybermenaces. Les modèles peuvent être manipulés via des attaques adversariales, ou exposés à des risques d'exfiltration de données (Papernot et al., 2018). Les

environnements hybrides dans lesquels s'intègrent ces technologies nécessitent des stratégies de sécurité renforcées, notamment pour les modèles déployés en cloud.

4.4 Problèmes de gouvernance et responsabilité

L'IA soulève des questions fondamentales en matière de responsabilité : qui est juridiquement responsable en cas d'erreur d'un système automatisé ? Ces incertitudes juridiques compliquent l'adoption à grande échelle, en particulier dans des secteurs régulés comme la finance ou la santé (Dignum, 2019). L'absence de cadre clair nuit également à la mise en place d'une gouvernance éthique, pourtant essentielle pour aligner l'usage de l'IA avec les valeurs de l'organisation.

5 Gouvernance éthique et réglementation de l'intelligence artificielle

L'intégration de l'intelligence artificielle dans les systèmes de contrôle interne et de gestion des risques ne peut se faire sans une gouvernance adaptée, à la fois éthique, réglementaire et opérationnelle. Les défis liés à la transparence, à la responsabilité et à la sécurité exigent des cadres robustes pour encadrer le développement et l'usage de ces technologies.

5.1 Normes et recommandations internationales

Plusieurs organismes internationaux ont proposé des cadres de référence pour une IA responsable. L'**OCDE**, dès 2019, a formulé cinq principes pour une IA digne de confiance : inclusivité, transparence, robustesse, responsabilité et durabilité (OECD, 2019). L'**UNESCO**, de son côté, a adopté en 2021 une **Recommandation sur l'éthique de l'IA**, mettant l'accent sur le respect des droits humains, la diversité culturelle et l'équité (UNESCO, 2021).

En Europe, le **Règlement sur l'intelligence artificielle (AI Act)**, actuellement en cours d'adoption, propose une approche fondée sur le risque : plus une application d'IA est jugée critique (par exemple dans la justice ou la finance), plus les exigences en matière de transparence, de documentation et de supervision sont strictes (European Commission, 2021). Ce modèle est susceptible d'influencer fortement les cadres nationaux et les pratiques organisationnelles, y compris au Maroc.

5.2 Gouvernance des algorithmes dans les organisations

Au niveau interne, la gouvernance de l'IA implique la mise en place de **comités d'éthique**, de **chartes d'utilisation de l'IA** et de **procédures de validation des modèles**. Le concept d'**IA explicable** (Explainable AI ou XAI) devient ici central, en garantissant que les résultats algorithmiques peuvent être interprétés et justifiés (Adadi & Berrada, 2018). Cette exigence est cruciale dans les domaines à fort enjeu de conformité et de responsabilité, comme l'audit, le contrôle financier ou la conformité réglementaire.

L'adoption de principes éthiques n'est pas seulement une obligation morale : elle représente un **avantage concurrentiel** en renforçant la confiance des parties prenantes et en anticipant les évolutions réglementaires. Des auteurs comme Virginia Dignum appellent à une **co-construction des systèmes d'IA** impliquant les experts métiers, les juristes, les informaticiens et les usagers finaux (Dignum, 2019).

6 Études de cas sectorielles (Maroc et international)

L'analyse d'expériences concrètes permet de mieux comprendre les dynamiques d'implémentation de l'intelligence artificielle dans les systèmes de contrôle interne et de gestion des risques. Cette section présente trois

types de cas : les initiatives du secteur bancaire marocain, les projets dans les entreprises publiques marocaines, et des comparaisons internationales.

6.1 Secteur bancaire marocain

Le secteur bancaire marocain montre une adoption progressive de l'IA, notamment dans les domaines de la conformité, de la lutte contre la fraude et de la connaissance client (KYC). Des banques comme Attijariwafa Bank et Bank of Africa ont investi dans des systèmes de détection de fraude transactionnelle basés sur l'intelligence artificielle (Attijariwafa Bank, 2023). Ces systèmes permettent une surveillance en temps réel et une réduction significative des faux positifs, tout en s'alignant avec les recommandations de Bank Al-Maghrib sur la digitalisation des processus de gestion des risques (Bank Al-Maghrib, 2023).

Cependant, ces initiatives restent limitées par un manque de ressources humaines spécialisées et une faible intégration des algorithmes dans les processus de décision à forte sensibilité (octroi de crédit, évaluation de risque systémique).

6.2 Grandes entreprises publiques marocaines

Des entreprises comme l'OCP (Office Chérifien des Phosphates) et l'ONCF (Office National des Chemins de Fer) ont développé des projets pilotes intégrant des systèmes d'IA pour la maintenance prédictive et la gestion des anomalies (OCP Group, 2022). Dans le cas de l'OCP, l'IA est utilisée pour anticiper les défaillances des équipements critiques, réduisant ainsi les interruptions de service et améliorant la conformité aux normes ISO en matière de sécurité et d'environnement.

Toutefois, le lien entre ces innovations et les dispositifs formels de contrôle interne reste encore flou. Les données générées sont rarement intégrées dans les matrices de risque ou les plans d'audit internes, faute d'un cadre de gouvernance numérique adapté.

6.3 Comparaison internationale

À l'échelle internationale, certains pays ont développé des stratégies IA robustes, intégrant explicitement la gouvernance des risques :

- **Canada** : Les institutions financières utilisent l'IA pour automatiser les audits, tout en respectant les lignes directrices du Bureau du surintendant des institutions financières (BSIF) en matière de gestion des risques technologiques (OSFI, 2022).
- **France** : La Cour des comptes française a expérimenté des outils d'analyse automatisée pour l'audit des comptes publics, dans le cadre du programme « data science et contrôle » (Cour des comptes, 2022).
- **Singapour** : L'autorité monétaire (MAS) a établi des principes de gouvernance algorithmiques, intégrant l'IA dans les mécanismes de supervision financière, avec une forte insistance sur l'explicabilité et la transparence (Monetary Authority of Singapore, 2018).

Ces expériences démontrent que l'intégration réussie de l'IA dans le contrôle interne repose sur une articulation forte entre innovation technologique, pilotage réglementaire et gouvernance éthique.

7 Recommandations et perspectives

À la lumière des apports et des limites identifiés dans les sections précédentes, plusieurs recommandations peuvent être formulées pour permettre une adoption raisonnée et durable de l'intelligence artificielle dans les dispositifs de contrôle interne et de gestion des risques.

7.1 Adapter les référentiels COSO et ISO à l'ère de l'IA

Les cadres existants, comme le COSO ERM ou la norme ISO 31000, restent pertinents, mais nécessitent une mise à jour pour intégrer explicitement les enjeux liés à l'IA : auditabilité des algorithmes, gestion des risques technologiques, gouvernance des données, etc. Des travaux récents proposent déjà des extensions aux modèles COSO pour y inclure la gestion des risques digitaux (Protiviti, 2021). Une telle adaptation permettrait aux organisations de structurer l'évaluation des risques liés à l'IA dans un langage cohérent avec les pratiques existantes.

7.2 Renforcer la formation des professionnels du contrôle

La montée en compétence des auditeurs internes, contrôleurs de gestion et risk managers est un impératif. Il est recommandé de développer des modules de formation continue intégrant des notions de machine learning, d'éthique algorithmique et de gouvernance technologique (IIA, 2020). Les institutions de formation professionnelle doivent adapter leurs référentiels pour inclure les enjeux liés à l'IA dans les cursus en audit, comptabilité et contrôle.

7.3 Promouvoir l'IA explicable et responsable (XAI)

L'utilisation de modèles interprétables (e.g. arbres de décision, modèles linéaires) ou de techniques d'explicabilité (SHAP, LIME) devrait être encouragée, notamment dans les secteurs réglementés (Molnar, 2022). L'implémentation d'une IA explicable renforce la confiance des utilisateurs et facilite les audits extrnes et internes. L'IA explicable permet également une meilleure appropriation des décisions par les équipes métier.

7.4 Mettre en place une gouvernance algorithmique

Une gouvernance efficace de l'IA suppose la création de structures internes de supervision : comités éthiques, rôles de "chief AI officer", processus de validation des modèles avant leur mise en production (World Economic Forum, 2021). Cette gouvernance doit inclure des mécanismes de redevabilité, de documentation des choix algorithmiques, et d'évaluation régulière des performances et des biais.

7.5 Intégrer l'IA dans une approche systémique de la gouvernance

Enfin, l'IA ne doit pas être vue comme un outil isolé, mais comme une composante d'un système global de gouvernance. Son intégration doit être alignée sur la stratégie globale, les valeurs de l'organisation, et les impératifs réglementaires. Cela nécessite une vision transversale, mobilisant des compétences multidisciplinaires (technologiques, juridiques, managériales) (Dignum, 2019).

8 Conclusion

L'intelligence artificielle s'impose comme un levier majeur dans l'évolution des dispositifs de contrôle interne et de gestion des risques. En permettant une analyse rapide et approfondie de données massives, en anticipant des scénarios de défaillance, et en automatisant des tâches à faible valeur ajoutée, l'IA représente une réponse efficace à la complexification croissante des environnements organisationnels.

Cependant, cette transformation soulève des défis de taille : biais algorithmiques, opacité des décisions, vulnérabilités en matière de cybersécurité, mais aussi des interrogations éthiques majeures quant à la transparence et la responsabilité des processus décisionnels automatisés. Ces limites doivent être prises en compte dès la conception des systèmes, dans une logique de gouvernance intégrée et de régulation proactive.

Les exemples nationaux et internationaux analysés dans cette communication montrent qu'une adoption réussie de l'IA repose sur plusieurs facteurs clés :

- l'adaptation des référentiels de gestion des risques (COSO, ISO),
- la formation des professionnels,
- l'usage de modèles explicables,
- et la mise en place d'une gouvernance algorithmique claire.

Il ne s'agit donc pas simplement d'introduire une nouvelle technologie, mais de repenser en profondeur les mécanismes de contrôle, la culture organisationnelle et les cadres de gouvernance. L'enjeu n'est pas technologique seulement, mais profondément humain et stratégique.

Ainsi, pour que l'IA contribue durablement à une gouvernance éthique et efficace, il est indispensable de conjuguer innovation technologique, vigilance réglementaire et responsabilité collective.

Pour prolonger cette dynamique et accompagner cette transformation, plusieurs perspectives méritent d'être envisagées. Il serait utile, d'une part, de capitaliser sur les retours d'expérience dans des contextes variés, notamment dans les structures de taille moyenne, encore peu préparées à ces transitions. D'autre part, l'élaboration de grilles d'évaluation spécifiques aux systèmes d'IA favoriserait une meilleure traçabilité, conformité et fiabilité. Une coordination renforcée entre les différents acteurs – métiers, techniques et juridiques – contribuerait à instaurer un climat de confiance. Enfin, cette évolution doit s'ancrer dans une démarche collaborative, fondée sur la participation active des parties prenantes. L'intelligence artificielle ne peut être imposée comme un simple outil ; elle doit être pensée comme un levier co-construit, au service d'une gouvernance durable et partagée.

REFERENCES

[1] Deloitte. *Risk management in the age of AI: How artificial intelligence is transforming risk practices*. Deloitte Insights; 2023.

[2] COSO. *Enterprise Risk Management - Integrating with Strategy and Performance*. Committee of Sponsoring Organizations of the Treadway Commission; 2017.

[3] Accenture. *AI for Risk and Compliance: Driving outcomes with intelligent technologies*. 2022.

[4] Binns R. Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. 2020;149-159.

[5] Russell S, Norvig P. *Artificial Intelligence: A Modern Approach*. 4th ed. Pearson; 2020.

[6] ISO. *ISO 31000:2018 - Risk Management — Guidelines*. International Organization for Standardization; 2018.

[7] COSO. *Internal Control—Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission; 2013.

[8] Goodfellow I, Bengio Y, Courville A. *Deep Learning*. MIT Press; 2016.

[9] Gunning D, Aha D. DARPA's Explainable Artificial Intelligence Program. *AI Magazine*. 2019;40(2):44–58.

[10] KPMG. *The Future of Internal Audit: Embracing Artificial Intelligence*. KPMG Insights; 2021.

[11] Deloitte. *AI and Internal Audit: Harnessing the Power of Artificial Intelligence*. Deloitte University Press; 2022.

[12] PWC. *Artificial Intelligence and Predictive Analytics in Risk Management*. PwC Report; 2020.IBM Institute for Business Value. *Auditing with AI: Intelligent Risk Assessment*. IBM; 2021.

[13] Campolo A, Sanfilippo M, Whittaker M, Crawford K. *AI Now Report 2017*. AI Now Institute; 2017.

[14] EY. *Digital Internal Audit: Applying Analytics and AI*. Ernst & Young Global; 2021.

[15] Barocas S, Selbst AD. Big Data’s Disparate Impact. *California Law Review*. 2016;104(3):671–732.

[16] Eubanks V. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin’s Press; 2018.

[17] Burrell J. How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*. 2016;3(1):1–12.

[18] Doshi-Velez F, Kim B. Towards A Rigorous Science of Interpretable Machine Learning. *arXiv preprint* arXiv:1702.08608. 2017.

[19] Papernot N, McDaniel P, Sinha A, Wellman M. SoK: Security and Privacy in Machine Learning. *IEEE European Symposium on Security and Privacy*. 2018.

[20] Dignum V. *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*. Springer; 2019.

[21] OECD. *OECD Principles on Artificial Intelligence*. OECD Legal Instruments; 2019.

[22] UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. United Nations Educational, Scientific and Cultural Organization; 2021.

[23] European Commission. *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. COM/2021/206 final.

[24] Adadi A, Berrada M. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*. 2018;6:52138–52160.

[25] Attijariwafa Bank. *Rapport annuel 2022*. Casablanca; 2023.

[26] Bank Al-Maghrib. *Rapport sur la supervision bancaire*. Rabat; 2023.

[27] OCP Group. *Digitalization and Predictive Maintenance Program*. 2022.

[28] OSFI (Office of the Superintendent of Financial Institutions). *Technology and Cyber Risk Management Guidelines*. Ottawa; 2022.

[29] Cour des comptes. *Audit et innovation numérique : Expérimentation de la data science*. Rapport public annuel; 2022.

[30] Monetary Authority of Singapore. *Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of AI and Data Analytics in Singapore's Financial Sector*. 2018.

[31] Protiviti. *Adapting COSO ERM for the Age of AI*. White Paper Series; 2021.

[32] IIA (Institute of Internal Auditors). *Artificial Intelligence – Considerations for theProfession of Internal Auditing*. Global Perspectives and Insights; 2020.

[33] Molnar C. *Interpretable Machine Learning*. 2nd ed. Leanpub; 2022.

[34] World Economic Forum. *Model Governance in AI: Guidelines and Best Practices*. Geneva; 2021.