

L'impact de l'intelligence artificielle sur le contrôle interne et la gestion des risques : opportunités, défis et recommandations

The Impact of Artificial Intelligence on Internal Control and Risk Management: Opportunities, Challenges, and Recommendations.

Auteur 1 : CHEGRI Soukaina

Auteur 2 : CHEGRI Meryem

Auteur 3 : EL-BAKKOURI Yasmine

CHEGRI Soukaina, ORCID : 0000-0002-8034-4158, Docteur,
Université Ibn Tofail, Faculté d'Economie et de gestion, Kénitra-Maroc.

CHEGRI Meryem, ORCID : 0000-0002-1826-5360, Docteur,
Université Ibn Tofail, Faculté d'Economie et de gestion, Kénitra-Maroc.

EL-BAKKOURI YASMINE, ORCID : 0009-0008-8990-209X, Doctorante,
Laboratoire de recherche en sciences de la gestion organisationnelle.
Université Ibn Tofail, Ecole Nationale de Commerce et de Gestion, Kénitra-Maroc.

Déclaration de divulgation : L'auteur n'a pas connaissance de quelconque financement qui pourrait affecter l'objectivité de cette étude.

Conflit d'intérêts : L'auteur ne signale aucun conflit d'intérêts.

Pour citer cet article : CHEGRI .S, CHEGRI .M & EL-BAKKOURI .Y (2026) « L'impact de l'intelligence artificielle sur le contrôle interne et la gestion des risques : opportunités, défis et recommandations », African Scientific Journal « Volume 03, Num 38 » pp: 001 – 020.



DOI : 10.5281/zenodo.23191167
Copyright © 2026 – ASJ



Résumé

L'intégration de l'intelligence artificielle (IA) dans le contrôle interne constitue un levier stratégique de modernisation des dispositifs de surveillance et de gestion des risques, cette dernière suscite un intérêt croissant, tant dans la littérature académique que dans la pratique professionnelle. En mobilisant l'apprentissage automatique, l'intelligence artificielle (IA) transforme profondément le paysage du contrôle interne et de la gestion des risques au sein des organisations. L'IA permet d'automatiser la détection des anomalies, d'anticiper les fraudes et d'optimiser la conformité réglementaire par une analyse continue de données massives. Notre recherche repose sur une revue systématique de la littérature conduite selon le protocole PRISMA. Cette contribution s'appuie sur une revue de littérature scientifique et professionnelle afin d'évaluer les apports concrets de l'IA aux fonctions de contrôle interne et la gestion des risques afin de proposer des recommandations pratiques pour atténuer les risques tout en maximisant les bénéfices.

Mots clés : Intelligence artificielle, contrôle interne, gestion des risques, digitalisation.

Abstract

Integrating artificial intelligence (AI) into internal control serves as a strategic lever for modernizing monitoring and risk management systems an area attracting growing interest in both academic literature and professional practice. By leveraging machine learning, AI is profoundly transforming the landscape of internal control and risk management within organizations. AI enables the automation of anomaly detection, fraud anticipation, and the optimization of regulatory compliance through the continuous analysis of big data. Our research is based on a systematic literature review conducted in accordance with the PRISMA protocol. This study draws on a review of scientific and professional literature to evaluate the tangible contributions of AI to internal control and risk management functions, aiming to offer practical recommendations for mitigating risks while maximizing benefits.

Keywords : Artificial intelligence, internal control, risk management, digitalization.

Introduction

La transformation digitale et l'intelligence artificielle ont grandement bouleversé le paysage des affaires au 21^e siècle, créant de nouvelles opportunités pour les organisations. Ces avancées, conjuguées avec la montée en puissance de l'IA, ont touché les processus opérationnels et décisionnels, ainsi que les méthodes de gestion des risques au sein des entreprises.

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)¹. 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). L'accélération de l'intégration des technologies d'IA dans les fonctions financières et opérationnelles pose des questions majeures pour le contrôle interne et la gestion des risques. Si l'IA promet une surveillance en temps réel et une meilleure détection des anomalies, elle introduit aussi des vulnérabilités nouvelles qui exigent une adaptation des cadres de contrôle traditionnel.

Au cœur de cette révolution technologique², l'intelligence artificielle (IA) occupe une place prépondérante, en modifiant non seulement les processus de gestion, mais aussi les pratiques de contrôle, tout en influençant de manière décisive la performance organisationnelle. Cependant, l'adoption croissante de l'intelligence artificielle au sein des organisations soulève des questions fondamentales concernant son véritable impact sur la performance organisationnelle, particulièrement dans le cadre des systèmes de contrôle interne. Il devient ainsi crucial d'explorer comment l'intelligence artificielle, couplée aux dynamiques de digitalisation, redéfinit les critères de performance dans des environnements de plus en plus complexes et volatiles.

La gestion des risques est une partie essentielle du processus commercial afin de maintenir l'efficacité de l'entreprise. Dans ce contexte, divers outils et technologies de sécurité et de gestion des risques sont mis en œuvre par les entreprises pour préserver la sécurité et la confidentialité des données. L'intelligence artificielle (IA) est de plus en plus intégrée dans les pratiques de gestion des risques des organisations publiques. Elle permet une analyse plus fine et plus rapide des

¹ MAAROUFI Abdelkader, & BRABIJE Hanane. (2025). L'Impact de l'Intelligence Artificielle sur le Contrôle Interne et la Gestion des Risques. *Revue Internationale De La Recherche Scientifique (Revue-IRS)*, 3(3), 2718–2727.

² BOUBOUHI et GHANIM M., (2024) « L'Intelligence Artificielle au Service du Contrôle Interne : Vers une Performance Organisationnelle Optimisée », *Revue Internationale des Sciences de Gestion* « Volume 7 : Numéro 4 » pp : 1346 -1369

données, ce qui est crucial pour identifier les risques et réagir de manière appropriée. Par exemple, l'adoption de l'IA dans la gestion des risques publics, telle que décrite par Bannister & Connolly (2020)³, a permis de structurer les cadres de gestion des risques pour minimiser les biais dans les algorithmes décisionnels, un enjeu majeur dans le secteur public.

Dans ce contexte, l'intelligence artificielle représente une étape encore plus ambitieuse dans cette transformation. En apportant des capacités d'analyse avancées, d'apprentissage automatique et de traitement en temps réel, l'intelligence artificielle va bien au-delà de la simple automatisation des processus. Selon Kaplan et Norton (1996), l'intelligence artificielle est capable de traiter des volumes massifs de données, d'analyser des tendances complexes, et de prendre des décisions basées sur des algorithmes prédictifs, ce qui peut améliorer considérablement la capacité d'une organisation à identifier et à gérer les risques dans ses systèmes de contrôle interne.

Généralement, le contrôle interne apparaît ainsi comme un outil essentiel pour garantir la fiabilité des informations financières, assurer la conformité réglementaire et renforcer la confiance des parties prenantes. En parallèle, la gestion du risque s'impose comme une démarche stratégique permettant d'identifier, d'évaluer et de maîtriser les incertitudes susceptibles d'affecter la pérennité des activités. À ces deux dimensions traditionnelles s'ajoute désormais l'essor de l'intelligence artificielle (IA), qui transforme profondément les pratiques de contrôle et de gestion. Grâce à ses capacités d'automatisation, d'analyse prédictive et de détection des anomalies, l'IA ouvre de nouvelles perspectives pour améliorer l'efficacité des dispositifs existants, tout en soulevant des enjeux éthiques et technologiques. En effet l'objectif général de notre étude et d'évaluer l'impact de l'intelligence artificielle (IA) sur les dispositifs de contrôle interne et de gestion des risques, en identifiant les opportunités qu'elle offre, les défis qu'elle soulève et les conditions d'une intégration maîtrisée.

L'intérêt de notre recherche est double premièrement, la littérature sur l'IA en audit et en contrôle interne reste fragmentée, entre travaux techniques (algorithmes de détection de fraude) et travaux managériaux. L'étude propose une synthèse structurée à l'intersection de ces champs. Elle identifie les lacunes de recherche et ouvre des pistes pour des études empiriques futures. Elle fournit des recommandations opérationnelles : gouvernance des modèles, supervision humaine, qualité des données, montée en compétences.

Cette recherche s'inscrit dans un positionnement épistémologique post-positiviste à orientation pragmatique, qui reconnaît l'existence d'une réalité organisationnelle observable, tout en admettant que sa connaissance reste partielle, située et médiatisée par les travaux antérieurs. L'objet étudié,

³ BOUBOUHI et GHANIM M., (2024) « L'Intelligence Artificielle au Service du Contrôle Interne : Vers une Performance Organisationnelle Optimisée », Revue Internationale des Sciences de Gestion « Volume 7 : Numéro 4 » pp : 1346 -1369

c'est-à-dire l'impact de l'intelligence artificielle sur le contrôle interne et la gestion des risques, relève d'un champ émergent, fragmenté et en évolution rapide, où les résultats empiriques demeurent dispersés entre travaux techniques et travaux managériaux. Dans ce contexte, une revue systématique de la littérature est apparue comme l'approche la plus adaptée. Elle permet de consolider des connaissances éparses selon une procédure explicite, transparente et reproductible (Tranfield et al., 2003)⁴, limitant ainsi les biais de sélection inhérents aux revues narratives traditionnelles. Le protocole PRISMA 2020 (Page et al., 2021)⁵ a été retenu pour structurer l'identification, le filtrage et l'inclusion des documents. Le raisonnement mobilisé est de nature abductive (Dubois et Gadde, 2002)⁶ : il procède par allers-retours entre les cadres théoriques existants (COSO, ISO 31000, modèle des trois lignes de l'IIA) et les données issues du corpus, afin de faire émerger des catégories d'analyse tout en les confrontant aux référentiels établis. Cette logique se traduit par une analyse de contenu thématique (Braun et Clarke, 2006 ; Mayring, 2014)⁷, à la fois déductive, par des axes préalablement définis (apports, risques, gouvernance), et inductive, par l'identification de thèmes émergents. Cette démarche qualitative vise moins à tester des hypothèses qu'à produire une synthèse interprétative rigoureuse, d'où découle un cadre de recommandations pratiques cohérent avec la visée pragmatique de l'étude, à savoir une connaissance utile à l'action des praticiens et des régulateurs. Ainsi, l'étude de l'impact du contrôle interne, de la gestion du risque et de l'intelligence artificielle permet de comprendre comment ces trois leviers, loin d'être indépendants, s'articulent pour renforcer la résilience et la compétitivité des organisations dans un environnement incertain. Cependant, cette technologie apporte également de nouvelles questions en matière de contrôle interne et la gestion des risques. C'est dans cette perspective que se situe la problématique centrale de cet article : Quel est l'impact de l'intégration de l'intelligence artificielle dans le processus du contrôle interne et de la gestion des risques ? Elle repose d'abord sur une revue critique de la littérature académique portant sur les interactions entre IA, contrôle interne et gestion des risques. Pour répondre à ces questions, Cet article présentera d'abord les concepts clés du contrôle interne, de la gestion des risques et de l'intelligence artificielle, puis il analysera les liens entre l'IA, le contrôle interne et la gestion des risques afin d'en identifier les limites et de proposer des recommandations.

⁴ Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), 207-222.

⁵ Page, M. J., McKenzie, J. E., Bossuyt, P. M., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71.

⁶ Dubois, A., & Gadde, L.-E. (2002). Systematic combining: An abductive approach to case research. *Journal of Business Research*, 55(7), 553-560

⁷ Mayring, P. (2014). Qualitative content analysis: Theoretical foundation, basic procedures and software solution.

1. Concept du contrôle interne

Le contrôle interne est un processus conçu et mis en œuvre par la direction et le conseil d'administration pour assurer la fiabilité des rapports financiers, la conformité aux lois et règlements, et l'efficacité des opérations, et il est toujours intégré dans la culture organisationnelle et vise à réduire les risques financiers et opérationnels Thomas, S. L. (2020)⁸. Selon Williams, G. D. (2018)⁹, le contrôle interne est comme un cadre de politiques et de procédures mis en place pour identifier, évaluer et gérer les risques dans le but d'assurer la réalisation des objectifs organisationnels, tout en garantissant la précision des rapports financiers et la conformité avec les règlements. D'après Hamilton, P. A. (2016) le contrôle interne est un processus continu, conçu par la direction pour assurer l'intégrité des rapports financiers, protéger les actifs contre les pertes, et promouvoir la conformité avec les lois et règlements. Cette définition souligne la nature continue et proactive du contrôle interne. Harris, M. J., & Drake, K.E. (2021)¹⁰ définissent le contrôle interne comme un processus mis en œuvre pour fournir une assurance raisonnable que les objectifs de l'organisation sont atteints, que les actifs sont protégés, que les informations financières sont fiables, et que les lois et règlements sont respectés. Ils mettent en lumière la manière dont le contrôle interne contribue à la gouvernance et à la gestion des risques. Richards, S. T. (2023) définit le contrôle interne comme un ensemble de processus technologiques et organisationnels destinés à garantir la sécurité des systèmes d'information, la précision des rapports financiers et la conformité aux normes régulatrices. Cette définition intègre les aspects numériques du contrôle interne.

Enfin, selon Miller et Xu (2023)¹¹, le contrôle interne ne peut offrir une garantie absolue de l'atteinte des objectifs, mais il constitue un outil essentiel pour minimiser les risques et maximiser l'efficacité opérationnelle. Ces études renforcent l'idée que le contrôle interne est non seulement un impératif réglementaire, mais aussi un levier stratégique pour la performance des établissements financiers. Ainsi, une mise en œuvre rigoureuse des mécanismes de contrôle interne peut conduire à une meilleure résilience face aux défis économiques et aux enjeux de conformité

⁸ Thomas, S. L. (2020). Internal Control and Corporate Governance : Ensuring Reliability and Compliance. *Journal of Accounting and Finance*, 20(3), 45–58.

⁹ Williams, G. D. (2018). Internal Control: Policies, Procedures, and Risk Management Frameworks. *Journal of Accounting and Organizational Change*, 14(3), 321–335

¹⁰ Harris, M. J., & Drake, K. E. (2021). *Internal Control Handbook*. International Finance Corporation (IFC), World Bank Group. Washington, D.C.

¹¹ TANGNIHO.M. F. & CHANHOUN.J.M. (2025) « Mécanismes de gouvernance et efficacité du contrôle interne dans les établissements financiers au Bénin », *Revue Française d'Économie et de Gestion* « Volume 6 : Numéro 2 » pp : 457-483.

1.1 La théorie de contingence

La théorie de la contingence, appliquée au contrôle interne digitalisé, postule que les structures et processus organisationnels doivent être adaptés en fonction de l'environnement externe et des spécificités contextuelles, particulièrement dans un contexte de digitalisation accrue. Selon cette théorie, les entreprises doivent concevoir des systèmes de contrôle interne flexibles qui répondent aux exigences spécifiques de leur environnement, permettant ainsi de mieux gérer les risques et opportunités engendrés par la transformation numérique (Donaldson, 2001). L'intégration des technologies numériques, telles que l'intelligence artificielle (IA) et les outils de gestion des risques en temps réel, renforce le contrôle interne en permettant une collecte de données plus rapide et une prise de décision fondée sur des analyses prédictives. Ce passage à la digitalisation améliore la résilience des entreprises, notamment en période de crise, en augmentant leur capacité de surveillance et en assurant une réactivité face aux défis externes, comme le soulignent Zhu et Song (2021) dans leur étude sur la performance des entreprises durant la pandémie de COVID-19. La théorie de la contingence nous rappelle que les entreprises doivent évaluer continuellement l'adéquation de leurs processus internes aux évolutions de leur environnement technologique pour garantir une performance optimale et la conformité réglementaire.

1.2 La théorie de la diffusion de l'innovation

La théorie de la diffusion de l'innovation, développée par Everett Rogers, décrit la manière dont une nouvelle idée, technologie ou pratique se propage au sein d'une société ou d'un groupe d'organisations est progressivement adoptée. Rogers identifie cinq étapes dans ce processus : (1) la connaissance, où les entreprises découvrent l'innovation ; (2) la persuasion, qui consiste à évaluer les avantages perçus ; (3) la décision ; (4) la mise en œuvre et (5) la confirmation, où l'innovation est intégrée et validée dans les processus organisationnels (Rogers, 2003). Rogers met également en lumière l'importance des leaders d'opinion et des canaux de communication dans la diffusion des innovations. Les entreprises influencées par des leaders d'opinion ou des pairs ayant déjà adopté des technologies de contrôle interne digitalisées sont plus enclines à franchir ce cap. Ce phénomène est corroboré par des études sur la transformation numérique en gestion des risques, où la pression concurrentielle et les exigences de conformité incitent les entreprises à adopter rapidement des outils digitaux (Zhu & Song, 2021)

1.3 La théorie de l'automatisation cognitive

La théorie de l'automatisation cognitive explore l'impact de l'intelligence artificielle (IA) sur les processus cognitifs en milieu professionnel, y compris le contrôle interne des entreprises. Cette approche repose sur l'idée que l'IA, en automatisant certaines tâches de traitement de l'information et de prise de décision, permet aux entreprises de repenser et d'optimiser leurs systèmes de contrôle

interne, leur conférant ainsi plus de précision et de réactivité (Kaplan & Haenlein, 2020). L'intégration de l'IA dans le contrôle interne transforme les mécanismes de surveillance et de conformité en introduisant des outils capables d'analyser de grandes quantités de données en temps réel, de détecter des anomalies et de prévoir des risques. Cette capacité d'automatisation de la détection et de l'analyse des risques réduit la dépendance aux processus manuels et permet aux contrôles internes de devenir plus adaptatifs et proactifs (Al-Htaybat & von Alberti-Alhtaybat, 2018). Davenport et Ronanki (2018) soulignent que ces systèmes d'IA facilitent la prise de décisions en minimisant les biais humains et en apportant des insights fondés sur des modèles prédictifs, rendant ainsi le contrôle interne non seulement plus précis, mais aussi plus stratégique.

2. Le contrôle interne : objectifs et composantes

Le contrôle interne est un pilier fondamental de la gouvernance organisationnelle, particulièrement dans les secteurs sensibles comme la banque. Il désigne l'ensemble des dispositifs, politiques, procédures et pratiques mis en œuvre pour maîtriser les risques, assurer la fiabilité de l'information et garantir la conformité aux réglementations en vigueur. Selon le référentiel international du COSO (Committee of Sponsoring Organizations of the Treadway Commission), le contrôle interne est défini comme : « Un processus mis en œuvre par le conseil d'administration, la direction et les autres personnels d'une entité, destiné à fournir une assurance raisonnable quant à la réalisation des objectifs suivants : efficacité et efficience des opérations, fiabilité de l'information financière » (COSO, 2013). Cette définition met l'accent sur la dimension systémique et intégrée du contrôle interne, qui ne doit pas être confondu avec le contrôle exercé a posteriori. Il s'agit d'un mécanisme proactif, transversal et évolutif, adapté aux spécificités de chaque organisation.

2.1 Objectifs du contrôle interne

Le contrôle interne est un système de gestion qui permet d'assurer l'efficacité et l'efficience des opérations, la fiabilité des informations financières et la conformité aux lois et réglementations applicables. Il est conçu pour aider les entreprises à atteindre leurs objectifs opérationnels, de reporting et de conformité¹².

Le contrôle interne poursuit trois objectifs principaux, complémentaires mais parfois en tension :

¹² OUTALEB Y. & LEMALEM A. (2023). « La transformation digitale et ses impacts sur les systèmes de contrôle interne : Etude des pratiques des entreprises marocaines », Revue du contrôle, de la comptabilité et de l'audit « Volume 7 : Numéro 4 », pp : 1- 26.

Tableau N°1 : les objectifs du contrôle interne

Objectifs	Description
Efficacité et efficience des opérations	Optimiser les processus internes pour atteindre les résultats stratégiques avec les ressources disponibles (Anthony & Govindarajan, 2007).
Fiabilité de l'information financière	Produire des données comptables et financières exactes, cohérentes et vérifiables.
Conformité aux lois et réglementations	Respecter les obligations légales, fiscales, prudentielles et déontologiques.

Source : Élaboration personnelle à partir de COSO (2013), Anthony & Govindarajan (2007)¹³.

En conclusion, les objectifs du contrôle interne sont liés aux opérations, à la conformité et au reporting. Ils visent à améliorer la qualité des opérations, à produire des informations financières fiables, à s'assurer de la conformité aux réglementations et à protéger les actifs de l'entreprise. Les entreprises doivent veiller à implémenter un contrôle interne efficace pour atteindre ces objectifs.

2.2 Les composantes du contrôle interne selon le COSO

Le contrôle interne est axé sur la réalisation d'objectifs dans un ou plusieurs domaines qui sont distincts, mais qui se recoupent. Il a pour fonction principale de mettre en place les dispositions afin de rendre les risques acceptables pour l'entreprise, de maîtriser ses activités et de clarifier la responsabilité de chacun (Gramet et al., 2008). L'efficacité du dispositif de contrôle repose sur la déclinaison de cinq composantes¹⁴.

Tableau N°2 : Les cinq composantes du contrôle interne selon le COSO

Composante	Définition et objectifs clés
1. Environnement de contrôle	Représente la culture organisationnelle, l'intégrité, les valeurs éthiques, la structure organisationnelle et la gouvernance (Simons, 1995).
2. Évaluation des risques	Identification et analyse des risques susceptibles de compromettre la réalisation des objectifs.

¹³ Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal Control – Integrated Framework. COSO, American Institute of Certified Public Accountants (AICPA).

¹⁴ BERRADA, M. (2020). Les fondements du contrôle interne comme dispositif anti-fraude. Revue Du contrôle, De La Comptabilité Et De l'audit, 4.

3. Activités de contrôle	Mise en place de politiques, procédures et vérifications pour réduire les risques à un niveau acceptable.
4. Information et communication	Assurer la circulation fluide, précise et en temps utile des informations nécessaires à tous les niveaux de l'organisation.
5. Pilotage (ou supervision)	Suivi, évaluation et ajustement continu du dispositif de contrôle interne.

Source : élaborer par nous-même

3. La gestion des risques

La gestion des risques (GR) est désormais considérée comme un pilier incontournable de la gouvernance, tant dans le secteur privé que dans le secteur public. Elle se définit comme un processus structuré et intégré visant à identifier, analyser, évaluer et traiter les incertitudes susceptibles d'affecter la réalisation des objectifs organisationnels (COSO, 2004 ; ISO, 2018)¹⁵. Dans le contexte des organisations publiques, la GR dépasse la simple protection contre les aléas : elle constitue également un levier de transparence, de responsabilisation et de performance (OCDE, 2014). Les définitions du risque abondent dans la littérature et varient selon les domaines. Le COSO (2004) insiste sur la survenance d'événements pouvant compromettre les objectifs stratégiques, tandis que l'ISO 31000 (2018) met en avant « l'effet de l'incertitude sur les objectifs », élargissant la notion aux opportunités. Pour leur part, l'AMF (2010, cité par Cordel, 2013) et l'IFACI (2010, cité par Renard, 2010) intègrent davantage les dimensions réputationnelles et de contrôle interne, essentielles dans les organisations publiques. Enfin, les contributions académiques soulignent la complexité et la dimension systémique du risque, en l'envisageant comme un ensemble dynamique d'interactions (Pignault & Magne, 2014 ; Amansou, 2019)¹⁶. La gestion des risques, également désignée par le terme anglais "Risk Management," a fait objet de nombreuses définitions dans la littérature¹⁷. (Bahamid et al, 2017) définit la gestion ou le management des risques comme étant « le processus systématique d'analyse, d'identification et de réponse aux risques. Elle consiste à maximiser les chances et l'impact des événements positifs tout en minimisant la probabilité et l'impact des événements négatifs, afin d'atteindre les objectifs ».

¹⁵ MONADI.I.&LAKRARSIA.(2025) « Modèle conceptuel de la relation entre gestion des risques, responsabilité des dirigeants et performance organisationnelle : Cas des fondations des œuvres sociales au Maroc », Revue Française d'Economie et de Gestion « Volume 6 : Numéro 10 » pp : 865 -878.

¹⁶ MONADI.I.&LAKRARSIA.(2025) « Modèle conceptuel de la relation entre gestion des risques, responsabilité des dirigeants et performance organisationnelle : Cas des fondations des œuvres sociales au Maroc », Revue Française d'Economie et de Gestion « Volume 6 : Numéro 10 » pp : 865 -878.

¹⁷ ACHIR. C et DOUARI. A. (2024) « Le management du risque à l'ère de l'émergence de l'intelligence artificielle », Revue Française d'Economie et de Gestion « Volume 5 : Numéro 1 » pp :52-77.

Cette définition nous invite à souligner que le risque peut revêtir un aspect positif ou négatif. Il peut être une opportunité, comme il peut être une menace induisant à une perte potentielle. Par ailleurs, la gestion des risques a un impact direct sur l'atteinte des objectifs de l'organisation. Selon Hopkin P. (2010), le risque est tout « événement ayant la capacité d'avoir un impact sur la mission, la stratégie, les projets, les opérations courantes, les objectifs, les processus de base, les dépendances clés et/ou la réalisation des attentes des parties prenantes ».

3.1 Processus de la gestion des risques

Le COSO ERM 2017 propose le processus de la gestion des risques comme suit¹⁸ :

- La gouvernance et la culture de gestion des risques : Cette étape consiste en la définition de la structure organisationnelle, les rôles et les responsabilités en matière de gestion des risques. Elle vise également à véhiculer une culture de gestion des risques dans l'organisation.
- La stratégie et l'objectif : Il s'agit d'inscrire la gestion des risques dans la stratégie globale de l'organisation, et de veiller sur la prise en compte des risques dans la définition des objectifs.
- L'identification des événements : Il s'agit du recensement des risques auxquels l'organisation est exposée, tout en prenant en considération les risques internes et externes.
- L'évaluation des risques : Le COSO fait appel à une évaluation qualitative et quantitative des risques à dessein de déterminer leur impact potentiel et leur probabilité.
- La réponse aux risques : Cette étape invoque la mise en place et le développement des stratégies de gestion des risques notamment la réduction, le transfert, l'acceptation ou l'évitement des risques.
- Les activités de contrôle : Il s'agit de mettre en place des contrôles internes dans le but de gérer les risques, surveiller les indicateurs de risque et d'apprécier l'efficacité des réponses aux risques.
- La communication et le reporting : Cette étape cruciale permet aux parties prenantes de prendre des décisions judicieuses et claires. La communication implique la création de rapports sur la gestion des risques.
- Le suivi et l'évaluation : Il s'agit de surveiller continuellement les risques, et de mettre le point sur la performance des réponses aux risques et de l'évolution de l'environnement des risques. Cela permet de rajuster les stratégies de gestion des risques si nécessaire.

¹⁸ ACHIR. C et DOUARI. A. (2024) « Le management du risque à l'ère de l'émergence de l'intelligence artificielle », Revue Française d'Economie et de Gestion « Volume 5 : Numéro 1 » pp :52-77.

- L'alignement de la gestion des risques avec la stratégie et la performance : Il convient de veiller que la gestion des risques est intégrée dans l'ensemble de l'organisation et qu'elle favorise l'atteinte des objectifs stratégiques.

Le processus de gestion des risques cherche à soutenir l'organisation dans sa quête vers la minimisation des pertes, la maximisation des opportunités et la prise des décisions éclairées.

3.2 Principes de la gestion des risques selon ISO 31000

La norme ISO 31000¹⁹, 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.

4. Définition et évolution de l'intelligence artificielle

L'intelligence artificielle (IA) désigne l'ensemble des théories, méthodes et technologies qui permettent à des machines d'accomplir des tâches normalement réservées à l'intelligence humaine, telles que la reconnaissance de formes, l'apprentissage, le raisonnement, la prise de décision ou encore le traitement du langage naturel (Russell & Norvig, 2016)²⁰.

Depuis sa naissance dans les années 1950, notamment avec les travaux de McCarthy, Minsky, Shannon et Turing, l'IA a connu plusieurs Phases de développement marquées par des périodes d'enthousiasme et de stagnation, appelées « hivers de l'IA ».

L'évolution de l'IA peut être structurée autour de trois grandes vagues²¹ :

- L'IA symbolique (1956-1980) : centrée sur des systèmes experts, cette phase visait à représenter les connaissances sous forme de règles logiques. L'approche reposait sur des algorithmes de type « si...alors », mais montrait rapidement ses limites face à des situations complexes ou incertaines (Newell & Simon, 1972).
- L'IA connexionniste (années 1980-2000) : inspirée du fonctionnement des réseaux de neurones biologiques, cette approche a redynamisé la recherche à travers les premiers

¹⁹ MAAROUFI Abdelkader, & BRABIJE Hanane. (2025). L'Impact de l'Intelligence Artificielle sur le Contrôle Interne et la Gestion des Risques. *Revue Internationale De La Recherche Scientifique (Revue-IRS)*, 3(3), 2718–2727.

²⁰ KHOULOUN., (2025) « L'intelligence artificielle au service du contrôle interne dans le secteur bancaire : Enjeux, opportunités et limites », *Revue du contrôle, de la comptabilité et de l'audit* « Volume 9 : numéro 2 » pp : 147-163

²¹ KHOULOUN., (2025) « L'intelligence artificielle au service du contrôle interne dans le secteur bancaire : Enjeux, opportunités et limites », *Revue du contrôle, de la comptabilité et de l'audit* « Volume 9 : numéro 2 » pp : 147-163.

modèles de réseaux neuronaux artificiels. Elle introduit les prémices de l'apprentissage automatique (Rumelhart, Hinton & Williams, 1986).

- L'IA basée sur l'apprentissage profond (depuis 2010) : portée par la puissance de calcul accrue, l'essor des mégadonnées (big data) et des algorithmes performants, cette phase a vu émerger l'intelligence artificielle dite « forte », capable de s'auto-améliorer par apprentissage à partir des données (Goodfellow, Bengio & Courville, 2016). Le deep learning, notamment les réseaux neuronaux profonds, a révolutionné des domaines comme la reconnaissance vocale, l'imagerie médicale, ou la détection de fraudes.
- L'IA moderne repose ainsi largement sur les techniques de machine learning, c'est-à-dire l'apprentissage statistique à partir de grandes masses de données, sans que l'intervention humaine ne soit nécessaire à chaque étape (Mitchell, 1997). Cette capacité d'auto-apprentissage permet aux systèmes d'identifier des régularités, de prédire des événements, voire de proposer des décisions automatisées, ce qui en fait un outil stratégique pour le secteur bancaire et la fonction de contrôle
- Du point de vue théorique, l'IA s'inscrit dans le courant technodéterministe (Beniger, 1986), selon lequel les évolutions technologiques conditionnent les transformations organisationnelles. Elle est également analysée dans le cadre de la théorie de la contingence (Galbraith, 1973), qui postule que les outils technologiques doivent s'adapter à la complexité et à l'incertitude de l'environnement pour améliorer la performance de l'organisation.

5. Impact de l'intelligence artificielle sur le contrôle interne

L'intégration de l'intelligence artificielle (IA) dans le contrôle interne transforme profondément la gestion des processus et la surveillance au sein des organisations. Selon la théorie de l'automatisation cognitive, l'IA améliore considérablement l'efficacité des contrôles internes en permettant de traiter de grandes quantités de données en temps réel et en réduisant le besoin d'audits manuels. Cette automatisation libère les équipes, leur permettant de se concentrer sur des tâches stratégiques à plus forte valeur ajoutée (Kokina & Davenport, 2017)²². De plus, l'IA renforce la précision des contrôles en détectant des anomalies et des schémas complexes, difficilement identifiables par des moyens traditionnels, ce qui contribue à limiter les erreurs humaines et à accroître la fiabilité des rapports financiers (Appelbaum, Kogan, & Vasarhelyi, 2017). La théorie de la diffusion de l'innovation soutient que l'IA favorise une amélioration continue des processus

²² Kokina, J., & Davenport, T. H. (2017). The Emergence of Artificial Intelligence : How Automation is Changing Auditing. *Journal of Emerging Technologies in Accounting*, 14(1), 115–122.

de contrôle grâce à ses capacités d'apprentissage adaptatif. Elle peut s'ajuster aux nouvelles menaces et évolutions réglementaires, assurant ainsi la pertinence des contrôles internes dans un contexte en perpétuel changement (Davenport & Ronanki, 2018). L'adoption de cette technologie est souvent encouragée par des dynamiques sociales et professionnelles, où l'influence des leaders d'opinion et la pression compétitive incitent les entreprises à intégrer des outils numériques pour rester performantes et conformes aux réglementations (Zhu & Song, 2021)²³. En parallèle, la théorie de la contingence souligne l'importance d'adapter les systèmes de contrôle interne à l'environnement technologique en évolution. L'impact de l'IA sur le contrôle interne va bien au-delà de l'amélioration opérationnelle, en apportant une réactivité accrue et en facilitant, parallèlement, la mise en œuvre de théories basées sur des modèles prédictifs. Cette transformation de la gestion des risques permet de réduire les coûts, tout en augmentant la rapidité et l'exactitude des processus de surveillance et de conformité. Kaplan et Haenlein (2020)²⁴ affirment que l'intégration de l'IA redéfinit l'architecture du contrôle interne, en permettant un passage d'une approche réactive à une approche proactive et prédictive, ce qui représente un impératif stratégique pour les organisations modernes. Finalement, en intégrant les perspectives des trois théories, il est évident que l'IA transforme le contrôle interne en augmentant l'efficacité, la précision et la réactivité des processus, tout en nécessitant une adaptation continue aux dynamiques de l'environnement technologique. Cette transformation stratégique renforce la position des organisations face aux défis contemporains, tout en maximisant les avantages de la digitalisation et de l'IA dans la gestion des risques et la conformité²⁵.

6. Relation entre l'intelligence artificielle et la gestion des risques

L'utilisation de l'IA a permis de développer un mode de vie moderne et de rendre la vie plus facile. Qu'il s'agisse d'affaires, de processus connexes ou d'activités domestiques quotidiennes, l'utilisation de l'IA a changé le mode de vie des individus. En outre, elle s'est révélée être une avancée technologique efficace. Toutefois, le développement des technologies permet de gérer les risques qui y sont associés (Papadaki et al., 2014). Dans ce contexte, la gestion des risques semble être un aspect important pour les entreprises afin de maintenir la confidentialité et la sécurité des données dans les processus commerciaux (Raza & Khosravi, 2015). En fait, pour chaque processus commercial, les entreprises suivent des stratégies efficaces de gestion des risques afin de réduire les risques technologiques et autres liés au processus commercial. Comme l'indiquent Pedrycz &

²³ Zhu, X., & Song, M. (2021). Digital transformation and firm performance : The role of adoption dynamics and competitive pressure. *Computers & Industrial Engineering*, 162, 107774.

²⁴ Kaplan, A., & Haenlein, M. (2020). Rulers of the world, unite! The challenges and opportunities of artificial intelligence. *Business Horizons*, 63(1), 37–50.

²⁵ BOUBOUHI et GHANIM M., (2024) « L'Intelligence Artificielle au Service du Contrôle Interne : Vers une Performance Organisationnelle Optimisée », *Revue Internationale des Sciences de Gestion* « Volume 7 : Numéro 4 » pp : 1346 -1369.

Chen (2015), la mise en œuvre de stratégies efficaces basées sur la gestion des risques au sein d'une organisation conduit à l'identification des attaques potentielles. Toutefois, l'identification des menaces avant l'attaque permet d'élaborer des stratégies d'amélioration. Comme l'affirment Gadre-Patwardhan et al. (2016), le développement d'une conception de réseau efficace par les entreprises permet de maintenir un réseau sécurisé pour les processus commerciaux, cela permet d'éviter les pertes de données et de préserver leur confidentialité. Selon Chen et al. (2020)²⁶, l'utilisation de l'IA dans plusieurs domaines a permis de développer le mode de vie des individus dans une large mesure. Cela a motivé les entreprises à explorer les avantages de l'intelligence artificielle. En outre, les entreprises peuvent améliorer leurs performances grâce à une mise en œuvre réussie de l'IA et éviter les risques qui y sont liés (Chen et al., 2020). La technologie peut mener à l'apparition des facteurs de risque dans le cas de manque de connaissance de celle-ci mise en œuvre. Comme le mentionnent Khodeir & Mohamed, (2015)²⁷, il existe différents risques liés à une mise en œuvre d'une technologie non maîtrisée. Selon Wu et al. (2014), les changements technologiques rapides et leur adoption par les entreprises sans connaissance adéquate des avancées technologiques créent un risque majeur pour les processus organisationnels. Le problème réside dans l'adaptation à la croissance technologique. S'il est vrai que l'idée des ordinateurs remplaçant les humains n'est pas encore concrétisée à grande échelle, il n'en reste pas moins que l'importance de l'adaptation à la croissance technologique s'est accrue au fil du temps (Wu et al., 2014). Cependant, cela a créé l'importance de la compréhension des technologies de l'IA afin de conserver l'efficacité de l'entreprise (Wu et al., 2014). C'est là que réside une relation majeure entre l'intelligence artificielle et la gestion des risques par les entreprises. Selon Kerzner là que les entreprises sont confrontées à un risque d'échec sur le marché en raison de divers facteurs. Ceux-ci comprennent une mauvaise connaissance de la technologie par les employés, une concurrence accrue sur le marché, des changements rapides dans la technologie, le maintien de la confidentialité des données, et d'autres encore. Dans le contexte de l'IA, le risque lié à la perte de données, au cryptage et au maintien de processus organisationnels structurés, réside dans les processus opérationnels²⁸.

²⁶ Chen, J., Wang, Y., & Zhang, X. (2020). Artificial Intelligence in Business: Applications, Risks, and Opportunities. *Journal of Business Research*, 116, 237–247.

²⁷ Khodeir, Laila M., and Ahmed H. Mohamed. "Identifying the Risks of Introducing New Technologies in Construction Projects." *HBRC Journal* 11, no. 2 (2015) : 129–135.

²⁸ KORCH &ERRAOUI. Théorie et application de l'intelligence artificielle dans la gestion des risques : Une revue de littérature *Revue AME* Vol 6, No 3 (Juillet, 2024) 165-183.

7. 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 dynamique²⁹.

- 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)³⁰. 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)³¹.
- Détection d'anomalies et analyse prédictive : L'analyse prédictive, alimentée par la 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).
- 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)³².
- 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

²⁹ MAAROUFI Abdelkader, & BRABIJE Hanane. (2025). L'Impact de l'Intelligence Artificielle sur le Contrôle Interne et la Gestion des Risques. *Revue Internationale De La Recherche Scientifique (Revue-IRS)*, 3(3), 2718–2727.

³⁰ KPMG (2021). *Future of Internal Audit : Harnessing the Power of Artificial Intelligence and Automation*. KPMG International.

³¹ Deloitte (2022). *The Robots Are Ready : Robotic Process Automation (RPA) and Artificial Intelligence in Internal Audit*. Deloitte Insights.

³² Campolo, A., Sanfilippo, M., Whittaker, M., & Crawford, K. (2017). *AI Now Report 2017*. AI Now Institute, New York University.

évolution vers des systèmes intelligents favorise une gouvernance adaptative, plus résiliente face aux changements environnementaux (EY, 2021)³³.

8. Les limites et les recommandations

8.1 Les limites

- Opacité et explicabilité : les équipes d’audit et de conformité peinent à interpréter certaines décisions algorithmiques.
- Biais et erreurs de données : modèles entraînés sur données historiques reproduisent biais et génèrent risques discriminatoires ou de mauvaise évaluation.
- Dépendance technologique et risques fournisseurs : concentration des fournisseurs d’IA et risques liés à la chaîne d’approvisionnement.
- Compétences et changement organisationnel : manque de compétences internes et résistance au changement freinent l’efficacité des implémentations.
- Politique de transparence et explicabilité adaptée au public interne et aux régulateurs.
- Plan de continuité et de gestion des fournisseurs (SLAs, audits fournisseurs).

8.2 Les recommandations pratiques

- Mettre en place une unité transversale IA–Risque–Conformité pour superviser les implémentations.
- Adapter les référentiels COSO et ISO à l’ère de l’IA
- Prioriser les cas d’usage à impact élevé/complexité faible pour des gains rapides (ex. détection d’anomalies).
- Déployer des indicateurs de performance des modèles et tableaux de bord de risque.
- Former les équipes de contrôle aux principes d’IA, biais et tests de robustesse.
- Renforcer la formation des professionnels du contrôle
- Intégrer l’IA dans une approche systémique de la gouvernance
- Intégrer clauses contractuelles relatives à la gouvernance des modèles dans les contrats fournisseur.

³³ EY, and European Commission, Directorate-General for Justice and Consumers. Study on the Relevance and Impact of Artificial Intelligence for Company Law and Corporate Governance: Final Report. Luxembourg : Publications Office of the European Union, 2021.

Conclusion

L'intelligence artificielle a le potentiel de renforcer significativement le contrôle interne et la gestion des risques en améliorant la détection, l'efficacité et la surveillance continue. Toutefois, sans gouvernance adaptée, contrôle des données et mécanismes d'audit des modèles, ces technologies peuvent introduire des risques nouveaux et complexes. Les organisations doivent équilibrer innovation et prudence, en adoptant des cadres de gouvernance, des pratiques de validation robustes et un renforcement des compétences internes.

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.

En définitive, loin de remplacer le jugement humain, l'intelligence artificielle doit être envisagée comme un amplificateur des capacités de contrôle, capable d'outiller les métiers du risque et de l'audit face à la complexité croissante de l'environnement. C'est à cette condition que l'IA pourra devenir un vecteur de pérennité, au service de la stabilité du système financier marocain. 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.

À cet égard, il est donc recommandé aux dirigeants de développer une vision stratégique qui intègre l'IA et la digitalisation dans le contrôle interne. Pour ce faire, les organisations doivent adopter une approche proactive, en investissant dans des solutions technologiques robustes tout en cultivant des compétences internes pour gérer les nouvelles dynamiques générées par l'intelligence artificielle. En outre, il est crucial d'établir une gouvernance claire pour assurer la transparence, la conformité et la responsabilité des systèmes intégrés.

En conclusion, si l'intelligence artificielle et la digitalisation ouvrent des horizons nouveaux pour le contrôle interne et la gestion des risques, ces technologies exigent une approche équilibrée, intégrant à la fois l'innovation technologique et la gestion humaine des processus. L'avenir du contrôle interne dépendra de cet équilibre délicat, où l'humain et la machine coexistent pour renforcer la résilience et la compétitivité des entreprises dans un environnement numérique en perpétuelle évolution.

BIBLIOGRAPHIE

ACHIR. C et DOUARI. A. (2024) « Le management du risque à l'ère de l'émergence de l'intelligence artificielle », Revue Française d'Economie et de Gestion « Volume 5 : Numéro 1 » pp :52–77.

BERRADA, M. (2020). Les fondements du contrôle interne comme dispositif anti-fraude. Revue Du contrôle, De La Comptabilité Et De l'audit, 4.

BOUBOUHI.et GHANIM M., (2024) « L'Intelligence Artificielle au Service du Contrôle Interne : Vers une Performance Organisationnelle Optimisée », Revue Internationale des Sciences de Gestion « Volume 7 : Numéro 4 » pp : 1346 -1369.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Internal Control – Integrated Framework. COSO, American Institute of Certified Public Accountants (AICPA).

Campolo, A., Sanfilippo, M., Whittaker, M., & Crawford, K. (2017). AI Now Report 2017. AI Now Institute, New York University.

Chen, J., Wang, Y., & Zhang, X. (2020). Artificial Intelligence in Business: Applications, Risks, and Opportunities. Journal of Business Research, 116, 237–247.

Deloitte (2022). The Robots Are Ready: Robotic Process Automation (RPA) and Artificial Intelligence in Internal Audit. Deloitte Insights.

Dubois, A., & Gadde, L.-E. (2002). Systematic combining: An abductive approach to case research. Journal of Business Research, 55(7), 553-560.

EY, and European Commission, Directorate-General for Justice and Consumers. Study on the Relevance and Impact of Artificial Intelligence for Company Law and Corporate Governance : Final Report. Luxembourg : Publications Office of the European Union, 2021.

Harris, M. J., & Drake, K. E. (2021). Internal Control Handbook. International Finance Corporation (IFC), World Bank Group. Washington, D.C.

Kaplan, A., & Haenlein, M. (2020). Rulers of the world, unite! The challenges and opportunities of artificial intelligence. Business Horizons, 63(1), 37–50.

Khodeir, Laila M., and Ahmed H. Mohamed. (2015) “Identifying the Risks of Introducing New Technologies in Construction Projects.” HBRC Journal 11, no. 2 (2015) : 129–135.

KHOULOUN., (2025) « L'intelligence artificielle au service du contrôle interne dans le secteur bancaire : Enjeux, opportunités et limites », Revue du contrôle, de la comptabilité et de l'audit « Volume 9 : numéro 2 » pp : 147-163.

Kokina, J., & Davenport, T. H. (2017). The Emergence of Artificial Intelligence: How Automation is Changing Auditing. Journal of Emerging Technologies in Accounting, 14(1), 115–122.

- KORCH &ERRAOUI (2004). Théorie et application de l'intelligence artificielle dans la gestion des risques : Une revue de littérature Revue AME Vol 6, No 3 (Juillet, 2024) 165-183.
- KPMG (2021). Future of Internal Audit: Harnessing the Power of Artificial Intelligence and Automation. KPMG International.
- MAAROUFI Abdelkader, & BRABIJE Hanane. (2025). L'Impact de l'Intelligence Artificielle sur le Contrôle Interne et la Gestion des Risques. Revue Internationale De La Recherche Scientifique (Revue-IRS), 3(3), 2718–2727.
- Mayring, P. (2014). Qualitative content analysis: Theoretical foundation, basic procedures and software solution. Klagenfurt.
- MONADI.I.&LAKRARS.I.A.(2025) « Modèle conceptuel de la relation entre gestion des risques, responsabilité des dirigeants et performance organisationnelle : Cas des fondations des œuvres sociales au Maroc », Revue Française d'Economie et de Gestion « Volume 6 : Numéro 10 » pp : 865 -878.
- OUTALEB Y. & LEMALEM A. (2023). « La transformation digitale et ses impacts sur les systèmes de contrôle interne : Etude des pratiques des entreprises marocaines », Revue du contrôle, de la comptabilité et de l'audit « Volume 7 : Numéro 4 », pp : 1- 26.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., et al. (2021). The PRISMA 2020 statement : An updated guideline for reporting systematic reviews. BMJ, 372, n71.
- TANGNIHO.M. F. & CHANHOUN.J.M. (2025) « Mécanismes de gouvernance et efficacité du contrôle interne dans les établissements financiers au Bénin », Revue Française d'Économie et de Gestion « Volume 6 : Numéro 2 » pp : 457-483.
- Thomas, S. L. (2020). Internal Control and Corporate Gouvernance : Ensuring Reliability and Compliance. Journal of Accounting and Finance, 20(3), 45–58.
- Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. British Journal of Management, 14(3), 207-222.
- Williams, G. D. (2018). Internal Control: Policies, Procedures, and Risk Management Frameworks. Journal of Accounting and Organizational Change, 14(3), 321–335.
- Zhu, X., & Song, M. (2021). Digital transformation and firm performance: The role of adoption dynamics and competitive pressure. Computers & Industrial Engineering, 162, 107774.