Revue du Contrôle de la Comptabilité et de l'Audit
ISSN : 2550-469X
Volume 9 : numéro 2

L'intelligence artificielle au service du contrôle interne dans le secteur bancaire : Enjeux, opportunités et limites

Artificial intelligence in the service of internal control in the banking sector: Challenges, opportunities and limits

KHOULOU Nahid (PhD Student)

Doctorante

Faculté des sciences juridiques économiques et sociale d'agadir

Université IBN ZOHR

Laboratoire des recherches en entrepreneuriat, finance et management des organisations (LREFMO), Maroc

Date de soumission : 03/05/2025

Date d'acceptation : 20/06/2025

Pour citer cet article :

KHOULOU N., (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.

Résumé

L'intégration de l'intelligence artificielle (IA) dans le contrôle interne bancaire constitue un levier stratégique de modernisation des dispositifs de surveillance et de gestion des risques. En mobilisant l'apprentissage automatique, 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. 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, tout en identifiant les limites et risques liés à son déploiement. Les principaux défis relèvent de la complexité technologique, de la protection des données, de l'éthique algorithmique et de l'évolution des normes réglementaires. Dans un environnement bancaire en transformation, l'IA s'impose ainsi comme un outil d'aide à la décision à fort potentiel, à condition qu'elle soit encadrée par une gouvernance adaptée et une vision stratégique claire.

Mots-clés : Intelligence artificielle, contrôle interne, secteur bancaire, conformité, gestion des risques, audit interne

Abstract

The integration of Artificial Intelligence (AI) into internal banking control represents a strategic lever for modernizing risk management and oversight mechanisms. Leveraging machine learning, AI automates anomaly detection, anticipates fraud, and enhances regulatory compliance through continuous analysis of large-scale data. This study is grounded in a review of scientific and professional literature, aiming to assess AI's concrete contributions to internal control functions while identifying the challenges inherent to its deployment. Key issues include technological complexity, data protection, algorithmic ethics, and the evolution of regulatory frameworks. In a rapidly transforming banking environment, AI emerges as a high-potential decision-support tool, provided it is implemented within a robust governance structure and aligned with a clear strategic vision.

Keywords : Artificial intelligence, internal control, banking sector, compliance, risk management, internal audit

Introduction

Le secteur bancaire est aujourd'hui en pleine mutation, confronté à une convergence de transformations technologiques, économiques et réglementaires. L'internationalisation des marchés, la montée en puissance des fintechs et néobanques, l'essor du big data, ainsi que la recrudescence des cybermenaces bouleversent les modèles traditionnels de gestion bancaire. Dans ce contexte, le contrôle interne devient un pilier essentiel de la résilience des établissements bancaires. Toutefois, les dispositifs classiques, souvent basés sur des procédures manuelles et des vérifications a posteriori, peinent à répondre aux exigences croissantes de rapidité, de précision et de proactivité.

Face à ces limites, l'intelligence artificielle (IA) émerge comme un levier stratégique de transformation des fonctions de contrôle. Elle permet l'automatisation des tâches répétitives, l'analyse prédictive des risques, la détection en temps réel des anomalies et une meilleure supervision des opérations. Dès lors, une question centrale se pose : dans quelle mesure l'IA peut-elle améliorer l'efficacité et la réactivité du contrôle interne dans le secteur bancaire tout en respectant les contraintes organisationnelles, éthiques et réglementaires ?

L'objectif de cet article est d'examiner les apports potentiels de l'IA dans les dispositifs de contrôle interne bancaire, mais aussi d'en analyser les limites et les conditions de succès. Il s'agit ainsi d'évaluer dans quelle mesure ces technologies peuvent transformer les pratiques actuelles, tout en répondant aux exigences de gouvernance, de cybersécurité et de conformité réglementaire.

En étudiant les travaux déjà effectués dans ce sujet et en se basant sur une revue de littérature,

On va tout d'abord dans une première section, définir les concepts clés relatifs à l'intelligence artificielle et au contrôle interne, en examinant leurs fondements théoriques ainsi que la manière dont ils interagissent dans le cadre bancaire. Dans une deuxième section, nous analyserons les opportunités offertes par l'intégration de l'intelligence artificielle au sein des dispositifs de contrôle interne, en mettant en lumière les gains potentiels en efficacité, en réactivité et en fiabilité. Enfin, une troisième section sera consacrée à l'étude des limites, défis et risques que peut engendrer cette transformation technologique, avant de conclure par une mise en perspective de la situation actuelle du secteur bancaire marocain face à ces mutations technologiques.

1. Fondements théoriques : Intelligence artificielle et contrôle interne

Dans cette première section, il convient de revenir sur les deux concepts fondamentaux de notre étude : l'intelligence artificielle (IA) et le contrôle interne, tout en mettant en lumière leur articulation dans un contexte bancaire.

1.1 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). 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 vagues :

- 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 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.
- Dans le secteur bancaire, l'intelligence artificielle est de plus en plus mobilisée pour optimiser la gestion des risques, détecter des opérations suspectes, automatiser les tâches comptables, ou encore renforcer la cybersécurité. Elle devient ainsi un acteur central du système de contrôle interne, capable de traiter des volumes massifs de données, de détecter des signaux faibles et d'alerter les responsables de conformité en temps réel (Appelbaum et al., 2017).
- Cependant, cette montée en puissance technologique soulève des interrogations quant à l'autonomie des systèmes, la fiabilité des modèles prédictifs, la transparence des algorithmes et la gouvernance de l'intelligence artificielle dans des environnements hautement régulés comme le secteur bancaire (Burrell, 2016 ; Jobin et al., 2019).

1.2 Le contrôle interne : rôle, 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.

1.3 Objectifs du contrôle interne

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

1.4 Le contrôle interne: rôle, 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 et conformité aux lois et règlements en vigueur. » (COSO, 2013)

- **Objectifs du contrôle interne**

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

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

- **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.
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

2. Revue de littérature

L'intelligence artificielle (IA) et le contrôle interne sont deux champs de recherche qui, bien que distincts dans leur origine, convergent de plus en plus dans les domaines de la gestion des risques, de l'audit, et plus largement dans la gouvernance bancaire. Cette convergence a suscité un intérêt croissant dans la littérature académique, surtout face aux transformations digitales qui bouleversent les pratiques de surveillance et de conformité dans les institutions financières.

2.1 Travaux sur l'intelligence artificielle appliquée au secteur financier

L'IA, dans son application au domaine bancaire, a été étudiée principalement sous les angles de l'efficacité opérationnelle, de l'automatisation des processus et de la gestion prédictive des risques. Plusieurs recherches ont montré que les technologies d'IA permettent de réduire les coûts opérationnels tout en améliorant la qualité des décisions financières (Brynjolfsson & McAfee, 2014 ; Davenport & Ronanki, 2018). Selon Vaidya et al. (2021), les algorithmes d'IA dans la banque sont capables de détecter des anomalies dans les flux financiers en temps réel.

Arner et al. (2017) mettent en avant l'émergence de la RegTech, qui permet de répondre aux exigences de conformité à travers des solutions automatisées basées sur l'IA.

2.2 Apports de l'IA au contrôle interne

Plusieurs auteurs ont exploré les apports de l'IA au contrôle interne. Issa et Kogan (2017) soulignent que l'IA permet de renforcer les activités de contrôle à travers l'automatisation des tâches répétitives, la génération automatique de rapports d'audit, et l'identification proactive des risques émergents. Appelbaum et al. (2017) montrent que les systèmes intelligents peuvent améliorer la qualité des audits internes et permettre une analyse continue, en adéquation avec les exigences de supervision constante dans le secteur bancaire.

2.3 Limites et défis identifiés dans la littérature

Malgré ses avantages, plusieurs limites à l'usage de l'IA dans le contrôle interne sont identifiées : le manque de transparence des algorithmes (Burrell, 2016), les risques éthiques liés aux données, la dépendance technologique excessive (Power, 2020), et l'inadaptation des structures de gouvernance. Munoko et al. (2020) insistent sur la nécessité d'un encadrement réglementaire et d'un contrôle humain complémentaire.

2.4 Synthèse des principales contributions académiques

Auteur(s)	Thème principal	Conclusion principale
Brynjolfsson & McAfee (2014)	IA et efficacité dans les entreprises	L'IA augmente la productivité et automatise les fonctions de gestion.
Issa & Kogan (2017)	Audit assisté par l'IA	Automatisation des tâches d'audit et détection des anomalies.
Arner et al. (2017)	RegTech et conformité bancaire	Réduction du coût de conformité grâce à l'IA.
Appelbaum et al. (2017)	Analyse continue dans l'audit	Surveillance renforcée et réduction des erreurs.
Burrell (2016)	Opacité algorithmique	Les IA sont difficiles à interpréter ('boîtes noires').
Munoko et al. (2020)	Éthique et gouvernance	Besoin de nouvelles règles éthiques et de supervision humaine.

Source : élaborer par nous-même à partir des publications cities.

3. Opportunités offertes par l'IA dans le contrôle interne bancaire

L'intégration de l'IA dans le contrôle interne bancaire ouvre un champ vaste d'opportunités en matière de performance, de conformité et de gouvernance des risques.

3.1 Automatisation et fiabilité des processus de contrôle

L'un des principaux apports de l'intelligence artificielle (IA) au contrôle interne réside dans sa capacité à automatiser un large éventail de tâches, améliorant ainsi la fiabilité, la rapidité et la cohérence des processus de surveillance et de vérification au sein des institutions financières. Cette automatisation transforme les pratiques classiques de contrôle, autrefois basées sur des procédures manuelles, en dispositifs intelligents capables d'analyser de grands volumes de données en temps réel.

3.2 Vers une automatisation des contrôles transactionnels

Traditionnellement, les contrôles internes reposaient sur des opérations de vérification ex post, souvent échantillonnées, et sujettes à l'erreur humaine. Grâce à l'IA, il est désormais possible de mettre en œuvre des contrôles automatisés en continu, intégrés directement aux systèmes d'information de l'entreprise. Ces contrôles sont en mesure de détecter instantanément les écarts, fraudes ou anomalies, sans intervention humaine.

Selon Appelbaum, Kogan et Vasarhelyi (2017), l'analyse automatisée des flux de transactions permet d'étendre la couverture du contrôle à 100 % des opérations, contrairement aux méthodes classiques basées sur des tests par sondage. Cela améliore considérablement la fiabilité du dispositif de contrôle.

3.3 Des algorithmes au service de la fiabilité

La fiabilité du contrôle repose également sur l'apprentissage automatique (machine learning), qui permet aux algorithmes de s'adapter aux évolutions des pratiques et des risques. Ces systèmes peuvent apprendre à identifier des schémas anormaux, à prédire des comportements frauduleux, ou à recommander des mesures correctives.

Davenport et Ronanki (2018) montrent que les entreprises utilisant l'IA dans le contrôle de gestion ou l'audit interne bénéficient d'une réduction significative des erreurs, d'un meilleur alignement sur les objectifs de conformité, et d'une réactivité accrue face aux risques émergents.

3.4 Exemples d'applications dans le secteur bancaire

Dans le secteur bancaire, plusieurs domaines du contrôle interne sont aujourd'hui partiellement ou totalement automatisés :

Domaine de contrôle	**Exemples d'automatisation IA**	**Bénéfices**
Contrôle des opérations clients	Analyse en temps réel des transactions suspectes	Réduction des fraudes, conformité réglementaire
Audit interne	Génération automatique de rapports d'audit	Gain de temps, couverture complète des données
Gestion des risques opérationnels	Identification prédictive des anomalies	Réduction des pertes, proactivité

Conformité réglementaire (KYC, AML)	Vérification automatisée des identités et suivi des flux financiers	Réduction des coûts, exactitude des vérifications

Source : élaborer par nous-même à partir de Appelbaum et al. (2017) et Vaidya et al. (2021)

- **Limites à considérer**

Malgré ces avancées, l'automatisation des contrôles soulève plusieurs défis :

- La dépendance aux données de qualité : des données erronées ou incomplètes peuvent entraîner de fausses alertes ;
- La compréhension limitée des décisions prises par les algorithmes (problème de boîte noire) (Burrell, 2016) ;
- La nécessité de surveillance humaine pour encadrer les résultats générés par les systèmes d'IA.

Ainsi, une automatisation réussie doit s'appuyer sur une stratégie hybride combinant technologies intelligentes et supervision humaine (Munoko et al., 2020).

3.5. Limites, risques et défis de l'IA dans le contrôle interne

- **Limites techniques et structurelles de l'IA**

Les systèmes d'IA, bien qu'avancés, présentent des failles technologiques. L'efficacité des algorithmes repose sur des données complètes, fiables et actualisées. Dans les environnements bancaires, les données sont souvent fragmentées entre systèmes, incomplètes ou biaisées (Zliobaite, 2017). Par ailleurs, les algorithmes complexes (comme le deep learning) produisent des décisions dont le raisonnement est difficile à interpréter (Burrell, 2016). Enfin, une IA formée sur des données historiques peut devenir obsolète dans des contextes changeants.

- **Risques juridiques, réglementaires et éthiques**

L'usage de l'IA soulève plusieurs préoccupations : la responsabilité juridique en cas d'erreur est floue (Wagner, 2018), et l'exploitation des données personnelles doit respecter des normes strictes comme le RGPD. Des biais algorithmiques peuvent également conduire à des discriminations non intentionnelles (O'Neil, 2016).

- **Défis humains et organisationnels**

L'introduction de l'IA dans le contrôle interne transforme les métiers. Certains professionnels perçoivent l'IA comme une menace pour leur emploi (Brougham & Haar, 2018). De plus, la rareté des profils hybrides et le manque de cadres de gouvernance adaptés ralentissent l'adoption efficace de ces technologies (Morley et al., 2020).

- **Enjeux pour une gouvernance maîtrisée de l'IA**

Pour encadrer l'usage de l'IA, il est recommandé de :

- Développer des algorithmes explicables (Explicable AI) ;
- Mettre en place un comité éthique IA ;
- Former les professionnels aux enjeux de IA ;
- Elaborer une charte de bonne utilisation de l'IA dans les dispositifs de contrôle.

- **Vers un contrôle interne intelligent : conditions de succès et perspectives dans le contexte marocain**

L'introduction de l'intelligence artificielle (IA) dans le contrôle interne bancaire marocain s'inscrit dans une logique de transformation digitale profonde, à la croisée des évolutions technologiques, des impératifs de régulation, et des attentes en matière de gouvernance. Cette mutation nécessite la mobilisation de plusieurs théories organisationnelles, technologiques et managériales, afin d'en comprendre les dynamiques et conditions de succès.

- **Conditions organisationnelles de réussite**

Théorie mobilisée : Théorie des capacités dynamiques (Teece, 2007)

Cette théorie stipule que les organisations doivent développer des capacités internes à détecter, saisir et reconfigurer les opportunités en environnement changeant. L'implémentation de l'IA dans le contrôle interne relève pleinement de cette logique.

A) Intégration stratégique

Les banques marocaines doivent intégrer l'IA non comme une innovation marginale mais comme un **levier stratégique de gouvernance** et de gestion des risques. Cela suppose un alignement entre projets technologiques et objectifs de contrôle.

B) Coopération interfonctionnelle

La mise en place de dispositifs IA nécessite une collaboration étroite entre directions de contrôle, de conformité, SI et data science. Cette synergie permet de concevoir des outils adaptés aux risques métiers.

C) Capital humain et apprentissage organisationnel

L'absence de compétences hybrides (maîtrise du risque et des technologies IA) est un frein majeur au Maroc. Les banques doivent investir dans la formation continue, les partenariats académiques (INSEA, EMI...), et la gestion du changement.

D) Gouvernance éthique

Dans un contexte de sensibilité éthique et réglementaire croissante, les banques doivent instaurer des comités d'éthique numérique, chartes algorithmiques, et indicateurs de confiance IA (ex. : traçabilité, explicabilité des décisions).

- **Cadre réglementaire et interopérabilité technologique**

Théorie mobilisée : Institutional Theory (DiMaggio & Powell, 1983)

Cette théorie explique que les organisations s'adaptent aux pressions institutionnelles (normatives, coercitives, mimétiques). Dans le cas marocain, la régulation bancaire influence fortement l'adoption de l'IA.

A) Cadre légal en évolution

Le Maroc dispose d'un socle réglementaire en matière de protection des données (loi 09-08), mais l'encadrement spécifique de l'IA dans les services financiers reste embryonnaire. Il est urgent que Bank Al-Maghrib élabore un cadre de référence sur l'IA appliquée au contrôle interne.

B) Pression normative croissante

Les exigences internationales (Bâle III, LBC-FT, IA Act UE...) influencent les régulateurs locaux. Le Maroc, en tant que membre du GAFI et partenaire de l'Union européenne, subit une pression pour harmoniser ses normes.

C) Interopérabilité des systèmes

L'IA exige des systèmes ouverts et compatibles, permettant le traitement transversal des données opérationnelles, financières et réglementaires. L'harmonisation des S.I. bancaires devient un enjeu stratégique.

- **Vers un contrôle prédictif et adaptatif**

Théorie mobilisée : Technological Acceptance Model (TAM) (Davis, 1989)

Le modèle TAM souligne que l'acceptation d'une technologie dépend de son utilité perçue et de sa facilité d'utilisation. Appliqué au contrôle interne, cela implique que les outils IA doivent être perçus comme fiables, compréhensibles et utiles.

A) Du contrôle a posteriori au contrôle en temps réel

L'IA permet de passer d'une logique de contrôle réactif à une surveillance continue et prédictive, à travers des alertes automatisées, des anomalies détectées en temps réel, ou encore des simulations de scénarios de risque.

B) Expérimentations locales et innovation ouverte

Des projets pilotes peuvent émerger via des incubateurs bancaires, des collaborations avec des fintech marocaines (via Fintech Maroc, UM6P Ventures, etc.), ou l'appel à des talents IA dans les grandes écoles.

C) Vers une architecture de contrôle intelligent

À terme, le système de contrôle interne pourra s'appuyer sur des modèles auto-apprenants, capables d'adapter les règles de détection en fonction du contexte. Cette logique renvoie au paradigme de « l'audit en continu », encore peu développé au Maroc mais porteur d'avenir.

Conclusion

L'intelligence artificielle redéfinit progressivement les contours du contrôle interne dans le secteur bancaire, en offrant des outils puissants d'analyse, d'automatisation et d'anticipation

des risques. Ce cas, observable à l'échelle mondiale, interpelle également le secteur bancaire marocain, en pleine mutation digitale et confronté à des exigences croissantes de transparence, de conformité et de résilience.

L'étude menée a permis de mettre en lumière trois dimensions fondamentales. D'abord, sur le plan théorique, la mobilisation de cadres comme la théorie des capacités dynamiques, la théorie institutionnelle ou encore le modèle d'acceptation technologique, a permis de structurer une lecture critique de l'intégration de l'IA dans les mécanismes de contrôle interne. Ensuite, sur le plan opérationnel, l'IA constitue un levier d'automatisation des processus de vérification, de fiabilisation des données et de prédiction des anomalies, marquant une rupture avec les méthodes traditionnelles. Enfin, sur le plan prospectif, l'étude a souligné les nombreuses conditions de réussite – humaines, organisationnelles, réglementaires et éthiques – sans lesquelles cette transformation ne pourrait s'inscrire dans la durée.

Pour le secteur bancaire marocain, l'IA représente un axe stratégique de modernisation du contrôle interne, à condition de dépasser une vision purement technologique et d'engager une démarche holistique fondée sur la gouvernance, la formation, l'innovation et la régulation. La réussite de cette transition dépendra de la capacité des banques à bâtir des environnements numériques de confiance, à encourager la coopération interdisciplinaire et à adapter les dispositifs de contrôle aux enjeux spécifiques du contexte marocain.

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 bancaire. C'est à cette condition que l'IA pourra devenir un vecteur de pérennité bancaire, au service de la stabilité du système financier marocain.

BIBLIOGRAPHIE

- Agence de Développement du Digital (ADD). (2023). Stratégie nationale pour l'intelligence artificielle au Maroc. Rabat : ADD. https://www.add.gov.ma
- Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement : Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1–27.
- Bank Al-Maghrib. (2022). Rapport annuel sur la supervision bancaire. Rabat : Bank Al-Maghrib. https://www.bkam.ma
- Banque Mondiale, & Bank Al-Maghrib. (2020). Digitalisation et inclusion financière au Maroc. Rabat : Banque mondiale.
- Basel Committee on Banking Supervision. (2010). Principles for enhancing corporate governance. Bank for International Settlements.
- CGEM – Confédération Générale des Entreprises du Maroc. (2021). Livre blanc sur la digitalisation et l'IA dans le secteur bancaire marocain. Casablanca.
- Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP). (2023). Loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. https://www.cndp.ma
- COSO – Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal Control – Integrated Framework.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160.
- Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining explanations: An overview of interpretability of machine learning. ArXiv. https://arxiv.org/abs/1806.00069
- HILMI, Y., & FATINE, F. E. (2022). The Contribution of internal audit to the corporate performance: a proposal of measurement indicators. International Journal of Performance and Organizations, 1(1), 45-50.

- HILMI, y., & NAJI, F. (2016). Audit social et performance de l'entreprise : une étude empirique au sein du champ organisationnel marocain. Revue des Etudes Multidisciplinaires en Sciences Economiques et Sociales, 1(3). doi:https://doi.org/10.48375/IMIST.PRSM/remses-v1i3.5271
- Hilmi, Y., & Fatine, F. E. (2022). Transformation digitale des cabinets d'audit par les réseaux sociaux: Cas de KPMG. International Journal of Economics and Management Sciences, 1(1).
- HILMI, Y. L'ÉTHIQUE DE L'ENTREPRISE: UN BON MOYEN DE PROTECTION CONTRE LA FRAUDE THE ETHICS OF BUSINESS: A GOOD WAY TO PROTECT AGAINST FRAUD.
- HILMI, Y. (2013). L'audit interne au Maroc: Degré d'intégration et spécificités de l'entreprise. Revue marocaine de recherche en management et marketing, (8).
- HILMI, Y. (2013). L'audit interne au Maroc: Degré d'intégration et spécificités de l'entreprise. Revue marocaine de recherche en management et marketing, (8).
- HILMI, Y., & Zakaria, E. Z. (2020). Contrôle interne de l'information financière et exigences de la loi Sarbanes-Oxley: Évaluation et proposition d'une démarche d'implémentation pour les entreprises marocaines. Revue du contrôle, de la comptabilité et de l'audit, 4(2).
- Hilmi, Y. (2014). Degré d'intégration de l'audit interne et performance des entreprises marocaines/cas de la région de rabat-sale-Zemmour-Zaïr.
- IIA – Institute of Internal Auditors. (2021). Global Internal Audit Standards. https://www.theiia.org
- Laftit, A. (2022). L'intelligence artificielle et la gouvernance financière : quels enjeux pour le Maroc ? Revue Marocaine de l'Audit et du Contrôle, 11(1), 67–82.
- Ministère de la Transition Numérique et de la Réforme de l'Administration. (2022). Feuille de route pour l'IA responsable au Maroc. Rabat.
- OECD. (2021). Recommendation of the Council on Artificial Intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
- Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. Strategic Management Journal, 28(13), 1319–1350.

- Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. Auditing: A Journal of Practice & Theory, 10(1), 110–125.