**Revue Internationale des Sciences de Gestion**
ISSN: 2665-7473
Volume 9 : Numéro 1

# L'adaptation des compétences de l'auditeur interne à l'ère du digital : entre exigences technologiques et éthique professionnelle

# Adapting Internal Auditors' Competencies in the Digital Era: Between Technological Demands and Professional Ethics

**OUHOUD Omar**
Doctorant Chercheur
Faculté des Sciences Juridiques, Économiques et Sociales
Université Cadi Ayyad
Innovations, Responsabilités et Développement Durable (INREDD)
Maroc

**EL OUAFA Khalid**
Enseignant Chercheur,
Faculté des Sciences Juridiques, Économiques et Sociales
Université Cadi Ayyad
Innovations, Responsabilités et Développement Durable (INREDD)
Maroc

**Date de soumission** : 09/01/2026

**Date d'acceptation** : 02/02/2026

**Pour citer cet article** :

OUHOUD O. & EL OUAFA K. (2026) « L'adaptation des compétences de l'auditeur interne à l'ère du digital : entre exigences technologiques et éthique professionnelle », Revue Internationale des Sciences de Gestion « Volume 9 : Numéro 1 » pp : 830 - 856

**Résumé**

Cet article examine l'adaptation des compétences de l'auditeur interne face à la transformation digitale (data analytics, RPA, IA/GenAI, cybersécurité) et ses implications éthiques. S'appuyant sur les Standards mondiaux de l'IIA (2024) et des travaux récents, il montre que la maîtrise technologique n'a de valeur que si elle demeure arrimée à l'intégrité, l'objectivité, la confidentialité et la diligence garanties par une supervision humaine structurée et un régime de preuve (pistes d'audit, fiches-modèles, journaux). L'étude propose une cartographie des compétences par rôles et articule la gouvernance des outils avec COSO/COBIT. Elle mobilise le cadre « trois couches » (gouvernance IT , audit du modèle, audit d'application) pour distinguer qualité technique et légitimité d'usage, et souligne la nécessité d'indicateurs d'impact (KPI) au-delà du simple suivi des licences. L'auditeur « hybride » qui conjugue technicité et jugement critique réduit le risque de non-détection et renforce la crédibilité de l'assurance dans l'économie digitale.

**Mots clés : Audit interne ; Compétences digitales ; IA/RPA ; Explicabilité ; Gouvernance (COSO/COBIT) ; Qualité d'audit/KPI.**

**Abstract**

This article analyzes how internal auditors' competencies must evolve amid digital transformation (data analytics, RPA, AI/GenAI, cybersecurity) and the resulting ethical implications. Building on the IIA Global Standards (2024) and recent scholarship, it argues that technological mastery only adds value when anchored to integrity, objectivity, confidentiality, and due professional care operationalized through structured human supervision and an auditable evidence regime (audit trails, model cards, execution logs). The study provides a role-based competency map and aligns tool governance with COSO/COBIT. It leverages a "three-layer" framework (provider governance, model audit, application audit) to distinguish technical quality from contextual legitimacy, and stresses impact metrics (KPIs) beyond mere license/usage tracking. The "hybrid" auditor combining technical fluency with critical judgment educes detection risk and strengthens the credibility of assurance in the digital economy.

**Keywords : Internal audit; Digital competencies; AI/RPA; Explainability; Governance (COSO/COBIT); Audit quality/KPIs.**

## Introduction

Dans un monde où la transformation digitale s'accélère à un rythme sans précédent, les organisations sont poussées à repenser leurs modèles opérationnels, leurs systèmes d'information et leurs pratiques de contrôle. L'émergence de technologies automatisées, telles que la robotisation des processus (RPA), l'analyse de données massives, ainsi que l'essor de l'intelligence artificielle générative (GenAI), impose de nouvelles exigences en matière de gouvernance, de transparence et de conformité (Vitali & Giuliani, 2024). Ces innovations remodèlent la nature de la fonction d'audit interne, traditionnellement centrée sur la conformité et le contrôle rétrospectif, en l'ouvrant vers un rôle plus proactif, axé sur la surveillance continue et l'anticipation des risques.

Dans ce contexte, l'audit interne n'est plus simplement un mécanisme correctif, mais devient un pilier central de la gouvernance digitale. Les parties prenantes direction générale, conseil d'administration, autorités de régulation attendent désormais des auditeurs internes qu'ils maîtrisent les outils technologiques, qu'ils interprètent les résultats des algorithmes et qu'ils assurent la fiabilité des processus automatisés (Liang et al., 2025). Cependant, cette exigence technique soulève une tension fondamentale : comment concilier la sophistication des compétences digitaux et le maintien du jugement éthique et professionnel, pierre angulaire de la crédibilité de l'audit ?

Cette tension est d'autant plus forte que les référentiels professionnels évoluent pour intégrer les défis du digital. Le référentiel de l'Institute of Internal Auditors (IIA) 2024 souligne spécifiquement les compétences requises en matière de technologie, tout en renforçant les obligations d'intégrité, d'objectivité, de diligence et de confidentialité. Pourtant, dans le contexte marocain et africain, peu de recherches ont examiné la façon dont les auditeurs internes peuvent développer des compétences digitales sans compromettre les exigences éthiques fondamentales.

Au regard de ce qui a été présenté, la question sous-jacente de notre travail de recherche alors est de savoir : **comment les compétences digitales exigées redéfinissent-elles le jugement éthique et professionnel de l'auditeur interne ?** Autrement dit, dans quelle mesure l'acquisition de compétences technologiques doit-elle être encadrée pour préserver le discernement, l'indépendance et la responsabilité de l'auditeur ?

Pour répondre à cette problématique, cet article poursuit trois objectifs premièrement cartographier les compétences technologiques clés attendues des auditeurs internes à l'ère du digital, deuxièmement articuler ces compétences aux exigences d'éthique et de

professionnalisme, telles que formulées dans le référentiel IIA 2024 troisièmement proposer un cadre conceptuel pour la formation, l'évaluation et la gouvernance de ces compétences hybrides dans les fonctions d'audit interne.

Pour atteindre ces objectifs, l'article s'organise comme suit. D'abord, une revue narrative et intégrative de la littérature récente, permettra d'identifier les compétences digitales les plus mobilisées telles que la data analytics, la visualisation avancée, l'automatisation/RPA, la cybersécurité et l'emploi de l'IA en s'appuyant notamment sur l'étude de Vitali & Giuliani (2024), qui examine l'impact des technologies émergentes sur les cabinets d'audit. Ensuite, nous analyserons comment ces compétences peuvent être associées aux principes d'éthique professionnelle notamment en ce qui concerne les biais algorithmiques, l'opacité des modèles, la responsabilité des décisions automatisées tout en maintenant le jugement du professionnel de l'audit.

Cette contribution se veut double, elle enrichit la littérature académique en comblant une lacune au carrefour des compétences digitaux et de l'éthique professionnelle en audit, et elle offre un outil conceptuel pratique aux directions d'audit, aux formateurs académiques et aux praticiens souhaitant aligner innovation technologique et rigueur professionnelle dans des contextes émergents. De plus, ce cadre ouvre des perspectives pour des études empiriques ultérieures, notamment dans le contexte marocain ou dans des secteurs industriels clés.

L'auditeur interne de demain sera un professionnel hybride, capable à la fois de maîtriser les technologies émergentes en questionnant les algorithmes, en validant la qualité des données et de préserver les principes fondamentaux du métier : intégrité, objectivité, discernement. Ce travail de recherche vise à offrir une structuration conceptuelle renouvelée pour ce double défi, en particulier dans les contextes africains où la digitalisation progresse à grande vitesse mais où les dispositifs de gouvernance technologique restent souvent embryonnaires.

## 1. Cadres référentiels et normatif

### 1.1. Évolution des référentiels professionnels

Depuis plus d'une décennie, la normalisation de l'audit interne a connu un mouvement de refonte visant à concilier l'exigence d'indépendance et de qualité avec l'irruption de technologies de plus en plus autonomes (data analytics, RPA, IA/GenAI). Ce mouvement culmine avec la publication des Global Internal Audit Standards (IIA, édition 2024), entrés en vigueur comme base des évaluations qualité à compter du 9 janvier 2025. Ces standards sont principes-centrés, structurés autour de 15 principes soutenus par des exigences, des

considérations de mise en œuvre et des exemples d'éléments probants, et ils replacent explicitement la compétence technologique et le professionnalisme éthique au cœur de la pratique. Cette nouvelle architecture dépasse l'ancienne logique du seul IPPF (2013/2017) pour proposer un cadre de référence davantage intégratif et évaluable, en prise directe avec la digitalisation rapide des organisations. IIA (2024)

Trois évolutions méritent d'être soulignées. Premièrement, la clarification de la finalité : les Standards réaffirment que l'audit interne « élève » la qualité de gouvernance en s'alignant sur les risques émergents, notamment digitaux, et en démontrant sa valeur à travers des résultats observables et traçables. Deuxièmement, la centralité des compétences : la notion de compétence ne se limite plus aux savoirs techniques traditionnels (comptables, juridiques ou procéduraux), mais englobe la maîtrise des technologies d'analyse de données, d'automatisation et d'IA, ainsi que la capacité à juger la qualité, la robustesse et l'éthique des outils mobilisés. Troisièmement, l'opérationnalisation par les « considérations de mise en œuvre » et les « exemples d'évidence de conformité », qui donnent aux départements d'audit une feuille de route concrète pour documenter la conformité et piloter la performance. IIA (2024)

Au cœur de cette refonte, le domaine « Ethics & Professionalism » fournit l'assise déontologique : intégrité, objectivité, confidentialité, diligence et compétence deviennent les garde-fous de l'audit à l'ère du digital. L'IIA précise que l'exercice du jugement professionnel n'est pas délégable aux outils ; il exige une supervision humaine de bout en bout, une traçabilité des raisonnements et une transparence sur les limites des modèles utilisés. La cartographie des termes et mappages « entre 2017 et 2024 » mise à disposition par l'IIA illustre comment ces exigences ont été modernisées et consolidées, en explicitant ce qui relève désormais d'un socle éthique commun et ce qui tient aux compétences digitales requises, y compris pour l'évaluation qualité externe (QAIP). (IIA 2024)

Cette évolution normative s'inscrit aussi dans un écosystème de cadres complémentaires. D'une part, l'agenda 2025 de l'audit interne (analyses globales des « hot topics ») souligne la montée en puissance de la GenAI dans les procédures d'audit (documentation, ciblage des tests, analyse de populations complètes) et appelle à de nouvelles compétences en cybersécurité et fraude. D'autre part, la littérature récente met en garde contre une routinisation non critique des outils , la performance perçue peut masquer des biais, une opacité des modèles et des lacunes de gouvernance si l'auditeur n'intègre pas des mécanismes d'explicabilité et d'auditabilité de l'IA. Ces constats justifient que les Standards 2024

insistent sur des exigences de planification stratégique, de gestion des talents et de mesure de performance adaptées au digital (Deloitte 2025).

Sur le terrain des guidances connexes, on observe une consolidation des attentes de gouvernance technique. Par exemple, la parution d'une guidance COSO pour encadrer la Robotic Process Automation (RPA) inscrit l'automatisation dans une logique de contrôle interne : objectifs, risques, contrôles, documentation et supervision indépendante. Pour l'audit interne, cela signifie que l'usage de RPA ne peut être considéré comme neutre ; il doit être gouverné, testé et documenté au même titre qu'une procédure sensible affectant la fiabilité de l'information. La normalisation converge ainsi vers un triptyque : outil > contrôle > assurance, dans lequel l'auditeur est à la fois utilisateur averti, évaluateur de contrôle et fournisseur d'assurance. COSO / The CPA Journal. (2025)

Parallèlement, la communauté académique propose des cadres d'audit de l'IA qui renforcent le socle normatif. Le modèle « three-layered approach » (gouvernance du fournisseur, audit du modèle, audit de l'application) décrit par Mökander et al. Montre comment articuler la gouvernance externe des modèles, la validation intramodèle et l'audit des usages organisationnels. Transposé à l'audit interne, ce cadre éclaire la séparation des responsabilités, l'équipe d'audit ne se substitue pas au développeur du modèle, mais vérifie la conformité des usages et l'intégration de garde-fous (explicabilité, données, robustesse). Cette articulation est cohérente avec l'esprit des Standards 2024, adopter l'innovation en gardant la primauté du jugement et de la responsabilité de l'auditeur, (Mökander et al 2024)

Enfin, l'évolution des référentiels s'accompagne d'une réinterprétation des compétences. La recherche empirique récente montre que la maturité des talents digitaux dans les équipes réduit les risques de détection et accroît l'efficacité de l'audit digitalisé, à condition d'être soutenue par une gouvernance claire des outils et des données. Cette convergence entre normes (IIA 2024/2025) et preuves empiriques suggère que l'alignement compétences éthique  technologies n'est pas un « plus » facultatif, mais un déterminant de qualité dans les missions modernes Liang, L (2025).

**Tableau 1 : De l'IPPF 2017 aux Standards 2024 : continuités et inflexions clés**

| Élément | IPPF 2017 | Standards IIA 2024 | Implication pratique |
|---|---|---|---|
| Architecture | Cadre modulaire centré normes/charte | 15 principes + exigences + considérations + exemples | Meilleure auditabilité de la conformité |
| Compétences | Accent technique traditionnel | Compétences digitales et éthiques explicitées | Plan de développement des talents structuré |
| Gouvernance techno | Peu explicitée | Intégration (data, RPA, IA) et supervision humaine | Traçabilité et explicabilité exigées |
| Qualité | QAIP lié au cadre IPPF | Évaluations qualité adossées aux 2024 Standards (eff. 09/01/2025) | Renforcement du pilotage de la performance |

**Source :** www.theiia.org

### 1.2. Enjeux éthiques liés à la digitalisation

La digitalisation de l'audit interne portée par l'analytique avancée, l'automatisation robotisée (RPA) et l'intelligence artificielle (IA, y compris l'IA générative) reconfigure la manière dont les preuves sont collectées, traitées et interprétées. Si ces technologies promettent une amélioration de l'efficacité et de la couverture des tests, elles introduisent simultanément de nouveaux risques éthiques qui touchent la fiabilité des résultats, l'indépendance du jugement et la confiance des parties prenantes. La littérature récente souligne que la transparence des systèmes, l'explicabilité des modèles et l'auditabilité des usages algorithmiques deviennent des conditions nécessaires pour maintenir l'intégrité de la pratique d'audit dans des environnements à forte intensité digital. À cet égard, l'IA & Society propose un cadre « à trois couches » distinguant l'audit de gouvernance (du fournisseur), l'audit du modèle (avant diffusion) et l'audit d'application (au niveau de l'usage organisationnel), afin d'éviter que l'auditeur ne confonde robustesse technique, conformité d'usage et responsabilité institutionnelle. Ce découplage analytique permet d'assigner clairement les responsabilités et d'ancrer l'évaluation éthique au plus près des risques réels rencontrés par la fonction d'audit Mökander et al (2024)

Un premier nœud éthique concerne les biais algorithmiques et leurs effets sur la qualité du jugement. Les modèles d'apprentissage, entraînés sur des données historiques, peuvent reproduire des discriminations latentes ou privilégier des modèles difficilement justifiables d'un point de vue professionnel. La littérature en Big Data & Society observe que les audits d'éthique de l'IA imitent les étapes des audits financiers, mais pêchent souvent par faible implication des parties prenantes, mesures de succès limitées et manque de reporting externe

autant de lacunes susceptibles d'amoindrir la crédibilité des dispositifs d'assurance sur les systèmes algorithmiques. Pour un auditeur interne, ces constats impliquent d'inclure, dans les plans d'audit, des tests dédiés à la non-discrimination, à la robustesse hors-échantillon et à la sensibilité aux variables proxy (par exemple, variables corrélées à des attributs protégés). (Schiff, D. S. 2024)

Un second enjeu tient à l'opacité des modèles et à l'explicabilité des résultats. L'usage de techniques complexes (transformers, ensembles, réseaux profonds) complique la traçabilité des liens entre données, paramètres et conclusions, alors même que la norme professionnelle exige de l'auditeur la capacité de justifier ses procédures et son jugement. Les travaux publiés dans *Frontiers in Human Dynamics* montrent que les audits algorithmiques et les évaluations d'impact constituent des instruments essentiels pour renforcer l'accountability des systèmes d'IA, en combinant mesures techniques, documentation des hypothèses et appréciation qualitative des risques. Il s'ensuit que la simple conformité fonctionnelle d'un modèle ne saurait suffire l'auditeur a intérêt à exiger des rapports d'explicabilité (feature importance, sensibilité locale, documentation des données) et des pistes d'audit qui relient les sorties algorithmiques aux assertions d'audit. (Cheong, B. C., et al. 2024).

La confidentialité et la protection des données constituent un troisième pilier éthique. L'intégration massive des données opérationnelles et financières dans des pipelines d'analytique et d'IA accroît l'exposition aux fuites, réidentifications et usages secondaires non autorisés. Les cadres proposés à l'ACM FAccT (2024) pour des audits d'assurance d'algorithmes insistent sur des critères explicitant la portée de l'audit (données, modèle, processus) et la collecte d'évidence (tests d'adversarialité, métriques quantitatives, entretiens, revues documentaires). Ce type d'approche, inspirée de l'audit financier, permet d'opérationnaliser la sécurité de l'information et la prévention des dérives dans les parcours de données, en clarifiant les responsabilités de contrôle (qui a accès, pour quoi faire, selon quelle journalisation) (Lam, K., et al. 2024).

Au plan déontologique, la digitalisation questionne la responsabilité morale et l'indépendance du jugement professionnel. L'automatisation à grande échelle peut induire une surconfiance dans les résultats outillés, au détriment de l'esprit critique. D'où la nécessité d'un principe de supervision humaine (« *human-in-the-loop* ») qui positionne l'auditeur comme gardien du sens , c'est à lui de qualifier les limites des modèles, d'apprécier la matérialité des écarts et de documenter le raisonnement professionnel reliant faits, contrôles et conclusion. La littérature récente en IA & Society souligne que ce rôle n'est crédible que si l'organisation distingue

l'assurance sur le modèle (robustesse, biais, performance) de l'assurance sur l'usage (adéquation aux objectifs d'audit, conformité au contexte, sécurité des données) distinction qui évite de confondre qualité technique et légitimité décisionnelle. (Mökander et al 2024)

Sur le plan organisationnel, l'éthique de la décision algorithmique appelle une gouvernance inter-fonctionnelle : l'audit interne, la conformité, l'IT/DSI et la direction des risques doivent co-construire des politiques qui encadrent l'acquisition, la validation, la mise en production et le retrait des outils digitaux. Les études récentes convergent sur l'idée qu'un audit crédible de l'IA suppose des métriques de performance et d'équité choisies ex ante, des revues indépendantes périodiques, et une traçabilité documentaire (fiches modèle, sources de données, journaux d'exécution). Cette approche réduit le risque d'« *ethics washing* » signalé par la littérature c'est-à-dire des proclamations éthiques non suivies d'effets vérifiables. (Schiff, D. S. 2024).

Enfin, la confidentialité des prompts et des contextes de travail avec des LLM impose des précautions spécifiques, séparation des environnements, masquage et pseudonymisation systématiques, et clauses contractuelles sur les droits d'usage des données d'audit par les fournisseurs de modèles. Ces pratiques, alignées avec les cadres d'audits d'assurance d'algorithmes, doivent être intégrées aux cartographies de risques de la fonction d'audit et assorties de tests de robustesse pour valider la résilience des dispositifs. (Lam, K., et al. 2024).

**Tableau 2 : Risques éthiques et mécanismes de mitigation**

| **Risque éthique principal** | **Manifestation en audit digitales** | **Mécanismes de mitigation** |
|---|---|---|
| Biais algorithmiques | Sélections d'échantillons ou scores à impact discriminant | Tests d'équité, analyses de sensibilité, implication des parties prenantes, reporting externe minimal (Schiff, 2024). |
| Opacité / non-explicabilité | Difficulté à justifier les conclusions assistées par IA | Rapports d'explicabilité, documentation des données et hypothèses, *model cards* (Cheong et al., 2024). |
| Confientialité / sécurité | Fuite ou réutilisation non autorisée de données d'audit | Critères d'ausdit d'assurance (portée, evidence), *adversarial testing*, traçabilité (Lam et al., 2024). |
| Confusion des responsabilités | Mélange « assurance modèle » / « assurance usage » | Cadre à trois couches (gouvernance, modèle, application) ; *human-in-the-loop* (Mökander et al., 2024), Kamar, R. et al 2024).. |
| Surconfiance dans l'automatisation | Affaiblissement du jugement professionnel | Revues indépendantes, seuils de matérialité revus, justification du raisonnement professionnel (Schiff, 2024). |

**Sources :** Schiff, (2024), Cheong et al., (2024), Lam et al., (2024), Mökander et al., (2024)

## 2. Compétences digitales de l'auditeur interne

### 2.1. Cartographie des compétences digitales

L'augmentation des usages de l'analytique, de l'automatisation robotisée (RPA) et de l'IA dans les organisations déplace le centre de gravité de la fonction d'audit, l'auditeur interne n'est plus seulement un « lecteur » de procédures et d'évidences, mais un acteur technique capable d'interroger des pipelines de données, de challenger des modèles et d'évaluer la robustesse des contrôles digitaux. Les publications récentes mettent en évidence trois traits structurants. Premièrement, la compétence digitale est multidimensionnelle : elle couvre la culture des données, la capacité d'automatiser des tests, la compréhension des modèles d'IA/ML, ainsi que la cybersécurité et la gouvernance de l'information. Deuxièmement, elle est située : la profondeur attendue varie selon le rôle (auditeur, responsable de mission, CAE) et le secteur d'activité. Troisièmement, elle est évaluable, les référentiels 2024 - 2025 insistent sur des niveaux de maîtrise observables et des mécanismes de preuve (documentation, traçabilité, indicateurs de performance). L'ensemble converge avec les Global Internal Audit Standards 2024 (Domaine II « Ethics & Professionalism »), qui exigent compétence, diligence et supervision humaine lors de l'usage d'outils digitaux, et replacent la responsabilité professionnelle de l'auditeur au-dessus des capacités techniques des systèmes. IIA (2024)

Sur le plan empirique, la littérature confirme que la maturité des talents digitaux est associée à des bénéfices tangibles. Une étude publiée dans *Scientific Reports* montre que l'adéquation des talents d'audit digital réduit le risque de non-détection (detection risk), via un effet direct et un effet médié par le degré de digitalisation des missions. Les auteurs soulignent toutefois un mécanisme complexe, si la digitalisation augmente la couverture et la vélocité des tests, elle peut simultanément accroître certaines expositions si la supervision et les contrôles de qualité ne sont pas renforcés d'où l'importance d'un pilotage par compétences et d'une gouvernance outillée (revues indépendantes, métriques d'explicabilité, cartographie des risques digitaux). (Liang, et al 2025)

Les cabinets et analyses professionnelles (2024–2025) convergent vers une liste canonique de domaines de compétence : (1) data analytics et visualisation, (2) IA/ML et GenAI, (3) RPA et automatisation des contrôles, (4) cybersécurité et résilience, (5) gouvernance des données et conformité, (6) communication des résultats data-driven. Les « hot topics » 2025 recensés par Deloitte GenAI en audit interne, fraude, cybersécurité, talents , confirment que l'élévation des compétences n'est pas un accessoire mais un préalable à des missions pertinentes et crédibles dans des environnements à forte intensité digitale. Deloitte. (2025) De même, les panoramas

KPMG/PwC insistent sur l'agilité de la fonction, l'upskilling continu et l'intégration de cadres de gouvernance de l'IA dans la planification d'audit. KPMG. (2024–2025), PwC. (2024).

Afin d'opérationnaliser cette pluralité, nous proposons la cartographie ci-dessous, inspirée des standards IIA (2024) et des tendances 2025. Elle distingue la finalité d'audit, les compétences clés, le niveau attendu et des évidences permettant d'attester de la maîtrise.

**Tableau 3 : Cartographie des compétences digitales de l'auditeur interne**

| Finalité d'audit | Compétence Digitale | Niveau attendu | Évidences de maîtrise |
|---|---|---|---|
| Étendre la couverture et la pertinence des tests | Data analytics & visualisation (ETL léger, SQL/Python, BI) | Intermédiaire >> Avancé | Scripts réutilisables, cahiers de tests datés, visualisations reliées aux assertions d'audit, *data lineage* documenté. |
| Challenger les preuves générées par systèmes | IA/ML & GenAI (principes, explicabilité, biais) | Fondamental >> Intermédiaire | Fiches-modèle, tests de sensibilité, justification des hyperparamètres pertinents pour l'audit, limites d'usage consignées. |
| Accélérer les procédures répétitives | RPA (conception/supervision de robots, contrôles) | Intermédiaire | Journalisation des exécutions, séparation des environnements, contrôles compensatoires et revues indépendantes. |
| Protéger l'intégrité et la disponibilité | Cybersécurité (contrôles d'accès, résilience SI) | Fondamental | Matrice d'accès auditée, tests d'intrusion coordonnés, revues de logs orientées risques. |
| Assurer la conformité et la qualité de l'info | Gouvernance des données (qualité, confidentialité) | Intermédiaire | Dictionnaire de données, règles de qualité, preuves de pseudonymisation/masquage, traçabilité RGPD/équivalents. |
| Renforcer l'impact auprès des parties prenantes | Communication data-driven (storytelling, matérialité) | Intermédiaire | Rapports avec annexes techniques, passerelles « résultats >risques > recommandations », traçabilité des décisions. |

**Sources :** IIA 2024 ; Deloitte 2025 ; KPMG 2025 ; PwC 2024

Deux éléments d'ingénierie des compétences sont décisifs pour éviter l'« illusion de maîtrise ». D'abord, l'ancrage déontologique : le Domaine II des Standards IIA exige que la compétence technique soit indissociable de l'intégrité, de l'objectivité, de la diligence et d'une supervision humaine explicite. Concrètement, l'auditeur trace son raisonnement (hypothèses, seuils, critères), documente la qualité des données (complet, exact, pertinent), et explicite les limites des méthodes employées. Ensuite, la gouvernance outillée : l'usage de

RPA ou d'IA doit être encadré par des politiques, des contrôles et des revues indépendantes (ex. guidance COSO pour la RPA), sous peine de déplacer le risque plutôt que de le réduire. IIA (2024)

La question des niveaux de maîtrise appelle une approche par rôles. Pour un auditeur, une maîtrise fonctionnelle (exécuter, interpréter, alerter) suffit souvent ; pour un chef de mission, on attend une capacité à concevoir des tests, à sélectionner des modèles adaptés aux objectifs d'audit et à arbitrer entre gain d'efficacité et risque d'opacité ; pour un CAE, il s'agit d'orchestrer la stratégie compétences-technologies, d'allouer les ressources (centre d'excellence data/IA, partenariats académiques), et d'établir des indicateurs de maturité (heures de formation, taux de réutilisation de scripts, profondeur d'explicabilité, fréquence des revues éthiques). Les analyses sectorielles 2025 (Deloitte/KPMG) confirment l'utilité d'une feuille de route compétences-risques alignée sur le plan d'audit, notamment dans les secteurs à forte criticité cyber ou à volumétrie transactionnelle élevée (Deloitte. 2025)

Enfin, la compétence digitale a une dimension collective. Les résultats empiriques suggèrent qu'elle réduit le risque de non-détection lorsque l'équipe dispose de talents digitaux adéquats et de pratiques de supervision adaptées (revues croisées, *human-in-the-loop*), alors que la digitalisation « à vide » peut induire des angles morts (sur-confiance, dérives d'usage). L'enjeu n'est donc pas de « technologiser » l'audit à tout prix, mais de rendre les auditeurs capables d'utiliser, d'expliquer et de contester les outils lorsque cela s'impose, en conservant la primauté du jugement professionnel. (Liang, et al 2025).

### 2.2. Transformation des rôles et profils

La transformation digitale déplace le rôle de l'auditeur interne d'un exécutant de procédures vers un conseiller « data-driven » capable de dialoguer avec les métiers et l'IT sur les modèles algorithmiques, la gouvernance des données et les contrôles automatisés. Des travaux récents montrent que l'adoption de technologies comme la RPA et l'IA reconfigure l'organisation des équipes, les pratiques de planification et la spécialisation des profils entre « constructeurs d'outils » et « challengers de modèles » (Vitali & Giuliani, 2024). Empiriquement, cette recomposition s'accompagne d'une redéfinition des compétences cœur (data analytics, IA explicable, gouvernance des données) et d'un renforcement de l'esprit critique pour arbitrer entre performance technique et matérialité des risques (Vitali & Giuliani, 2024).

Au niveau des équipes, l'émergence d'un vivier de talents digitaux est corrélée à une réduction du risque de non-détection via l'élévation du degré de digitalisation des missions,

mais aussi à une exposition accrue si la supervision n'est pas adaptée, la digitalisation augmente la vitesse et la couverture, tout en pouvant amplifier certains risques si la qualité n'est pas pilotée (Liang et al., 2025). L'étude montre un effet direct (les talents digitaux réduisent le risque) et un effet médié (la digitalisation peut, si mal encadrée, accroître l'exposition), d'où la nécessité de revues indépendantes et d'indicateurs d'explicabilité (Liang et al., 2025).

La montée en puissance des compétences digitaux est également associée à une qualité perçue supérieure des missions, à condition d'articuler les aptitudes techniques (manipulation de grands jeux de données, visualisation, compréhension des algorithmes) et les compétences créatives (formulation d'hypothèses, conception de tests, narration des résultats) (Al Frijat & Al-Hajaia, 2025). Cette combinaison « tech + design d'enquête » renforce la pertinence des travaux, optimise le ciblage des tests et améliore la communication des constats auprès des organes de gouvernance (Al Frijat & Al-Hajaia, 2025).

Sur le cycle d'audit, l'IA générative s'invite désormais du cadrage à la rédaction, en passant par la revue documentaire et l'élaboration de programmes de travail. Des enquêtes récentes dans la profession documentent des usages responsables de GenAI lorsque l'on maintient des garde-fous de gouvernance (politiques d'usage, données non sensibles, validation humaine) et des tests d'efficacité circonscrits à des cas d'usage faible matérialité (IIA Research Foundation, 2024). Dans cette configuration, la valeur ajoutée tient au gagné de productivité et à la qualité de synthèse, sans substitution du jugement professionnel (IIA Research Foundation, 2024).

La confidentialité des données et la conformité prennent une dimension stratégique à mesure que les auditeurs internalisent des pipelines d'analytique et d'IA. Des travaux en Journal of Information Systems soulignent que la provenance, la qualité et la protection des données constituent des déterminants de confiance et des sources de risque si elles sont négligées (Chen, Zhao & Wang, 2024). Pour l'audit interne, cela implique des profils capables de documenter la lignée des données, de configurer le masquage/pseudonymisation dans les environnements d'analyse et d'intégrer des tests de confidentialité dans les plans de mission (Chen et al., 2024).

Dans les grands cabinets et fonctions structurées, l'adoption de l'IA requiert des rôles différenciés : « product owners » d'outils, data scientists internes, auditeurs « méthode » et auditeurs « métier », avec une gouvernance claire des responsabilités (Kokina et al., 2025). Les analyses 2025 insistent sur des freins pratiques (qualité des données, explication des

modèles, responsabilité partagée) et des opportunités (ciblage des anomalies, couverture populationnelle, monitoring continu), ce qui milite pour des profils hybrides et des parcours d'upskilling gradués (Kokina et al., 2025).

La dimension éthique irrigue ces évolutions : la transformation des profils n'a de sens que si les auditeurs conservent la primauté du jugement, documentent la traçabilité et séparent l'assurance sur le modèle (robustesse, biais, performance) de l'assurance sur l'usage (adéquation au contexte, objectifs d'audit, sécurité des données). La littérature sur l'audit des modèles propose un cadre à trois couches (gouvernance du fournisseur, audit du modèle, audit d'application) qui éclaire la répartition des responsabilités et évite la confusion entre qualité technique et légitimité décisionnelle (Mökander, Schuett, Kirk & Floridi, 2024).

Conséquence organisationnelle, les fiches de poste évoluent vers des profils T-shape (profondeur analytique + largeur métier/éthique). Les responsables de mission doivent orchestrer la sélection des outils, l'explicabilité attendue, les seuils de matérialité et les revues indépendantes, tandis que les CAE portent la stratégie compétences (centres d'excellence data/IA, partenariats académiques, indicateurs de maturité) (Vitali & Giuliani, 2024 ; Kokina et al., 2025). Le développement continu (heures de formation ciblées IA/RPA/Privacy, certifications modulaires) devient un KPI de maturité autant qu'un levier de rétention des talents (Vitali & Giuliani, 2024 ; Kokina et al., 2025).

Enfin, la transformation des rôles est indissociable d'une communication data-driven vers les comités d'audit, traduire les sorties algorithmiques en assertions d'audit, expliciter les incertitudes et matérialiser les recommandations actionnables. Les études montrent que l'impact de l'audit s'accroît lorsque la compétence digitale se double d'un design de restitution clair (tableaux de bord, récits visuels) et d'un ancrage déontologique explicite (Al Frijat & Al-Hajaia, 2025 ; Liang et al., 2025). C'est cet équilibre, technicité, éthique, clarté, qui caractérise les nouveaux profils d'auditeurs internes performants à l'ère de l'IA (Al Frijat & Al-Hajaia, 2025 ; Liang et al., 2025).

### 2.3. Défis organisationnels

La digitalisation de l'audit interne révèle des frictions classiques ; inerties, routines, silos, que l'introduction d'outils data analytics, RPA et IA exacerbe. Elle reconfigure la division du travail entre « constructeurs » (développeurs de scripts/robots) et « challengers » (auditeurs qui testent et interprètent), bousculant frontières métiers et hiérarchies (Vitali & Giuliani, 2024). Sans design organisationnel clair (rôles, accès, responsabilités), ces outils peuvent

accroître les asymétries d'information et la dépendance à quelques experts, au détriment de l'apprentissage collectif. Le différentiel de compétences constitue un second verrou : des talents digitaux suffisants réduisent le risque de non-détection, mais une digitalisation mal encadrée peut multiplier des tests peu explicables, d'où la nécessité d'upskilling, de revues indépendantes et de supervision humaine (HITL) (Liang et al., 2025). Troisièmement, la gouvernance des données (provenance, intégrité, confidentialité) conditionne la validité des conclusions : traçabilité lacunaire, transformations opaques et exposition de données sensibles exigent data lineage, pseudonymisation et tests de confidentialité (Chen, Zhao & Wang, 2024).

Méthodologiquement, l'automatisation accroît la couverture et la vélocité, mais requiert plus d'efforts amont (sélection des signaux, paramétrage) et aval (validation/interprétation), ainsi qu'une re-planification en contrôle continu (Fang et al., 2025). Ces défis recoupent l'évolution normative : le Domaine II « Ethics & Professionalism » (IIA, 2024) impose de documenter la supervision humaine à chaque étape critique, tandis que l'IIA Competency Framework (2025) relie montée en compétences, stratégie d'audit et qualité. Enfin, la guidance COSO sur la RPA exige objectifs, évaluation des risques, journalisation et revue indépendante ; l'acculturation progresse via environnements sécurisés, cas d'usage à faible matérialité et formation incrémentale (COSO, 2025 ; Deloitte, 2024).

## 3. Technologies émergentes et redéfinition du jugement professionnel

### 3.1. Gouvernance des outils digitaux

La gouvernance des outils digitaux en audit interne exige d'articuler les référentiels de contrôle interne (COSO), de gouvernance des SI (COBIT), de management des risques (ISO/ISO-IEC) et les Standards professionnels de l'IIA, afin d'assurer une utilisation responsable et audit-able de l'automatisation (RPA) et de l'intelligence artificielle (IA). Les Global Internal Audit Standards (2024) posent le principe selon lequel l'usage d'outils ne transfère ni la responsabilité ni le jugement de l'auditeur : la fonction doit documenter la compétence, la diligence, la traçabilité et la supervision humaine, notamment au sein du Domaine II "Ethics & Professionalism" (IIA, 2024). Cette exigence place la preuve (evidence) au cœur du dispositif : fiches de modèle, journaux d'exécution, documentation des données et des limites, cartographies des risques digitaux, etc.

Sur le versant contrôle interne, la guidance COSO consacrée à la Robotic Process Automation (RPA) (2025) formalise un cadre de gouvernance intégrant objectifs, risques, contrôles,

journalisation et revues indépendantes. Elle rappelle que les robots  y compris lorsqu'ils soutiennent des tests d'audit doivent être conçus et opérés sous un ensemble de contrôles documentés, avec une séparation claire des environnements (développement/test/production) et une traçabilité des exécutions (COSO, 2025). Pour l'audit interne, cela implique de tester la conception (design) et l'efficacité opérationnelle (operating effectiveness) des automatismes comme n'importe quel contrôle clé, et d'adosser toute conclusion à une piste d'audit techniquement vérifiable (COSO, 2025).

Du côté gouvernance SI, COBIT fournit l'ossature pour aligner la technologie sur les objectifs d'affaires et répartir les responsabilités (comités, propriétaires de processus, fonctions d'assurance). Les publications ISACA 2025 explicitent comment COBIT peut être utilisé comme cadre pratique pour la gouvernance de l'IA : précision des decision rights, définition d'indicateurs (exactitude, responsabilité, supervision), intégration des pratiques d'assurance au cycle de vie des modèles (ISACA, 2025). En complément, les travaux 2024 soulignent que COBIT sert de boussole dans la transformation IA, en veillant à l'alignement sur les objectifs, à la conformité et à la gestion des risques (ISACA, 2024). Pour une fonction d'audit, l'intérêt est double : (i) disposer d'un vocabulaire commun avec l'IT/risques, (ii) cadrer des revues régulières (politiques, rôles, données, changements de modèle).

Sur le plan réglementaire et de supervision externe, la Financial Reporting Council (FRC) a publié en 2025 une guidance décrivant l'intégration d'un outil IA dans des procédures illustratives (ex. tests de journaux), avec des attentes de documentation et de justification des choix méthodologiques ; parallèlement, la FRC constate que les grands cabinets suivent encore insuffisamment l'impact de ces outils sur la qualité d'audit et les invite à définir des KPI de performance, d'éthique et d'efficacité (FRC, 2025). Pour l'audit interne, ces signaux renforcent l'idée que la gouvernance des outils digitaux doit inclure des mesures d'impact (qualité, couverture, faux positifs, délais), au-delà du simple suivi des licences ou usages.

L'IIA a, de son côté, publié en 2025 un Global Best Practice positionnant l'audit interne comme catalyseur d'une gouvernance robuste de l'IA : mise en place de comités de gouvernance multi-fonctions, identification des risques émergents, et développement de services d'assurance adaptés (IIA, 2025). Cette vision insiste sur la séparation entre assurance sur le modèle (qualité des données, équité, robustesse, explicabilité) et assurance sur l'usage (adéquation au contexte, sécurité des données, conformité aux politiques), distinction déjà soulignée dans la littérature académique et qui évite de confondre qualité technique et légitimité décisionnelle (IIA, 2025).

Opérationnellement, une toile d'alignement peut être mise en place : COSO pour l'efficacité des contrôles des automatismes (RPA et scripts d'audit), COBIT pour la gouvernance (rôles, politiques, cycle de vie, gestion des changements), IIA 2024 pour la responsabilité professionnelle (éthique, supervision humaine, traçabilité) et FRC pour l'évidence de qualité attendue en contexte d'audit (documenter les choix, expliciter l'usage, paramétrer des KPI). Cette inter-opérabilité crée un régime de preuve continu : chaque outil digital est relié à des objectifs, des risques, des contrôles, des responsabilités et des métriques ; chaque mission d'audit conserve la primauté du jugement, matérialisée par des revues indépendantes et une documentation explicite (IIA, 2024 ; COSO, 2025 ; ISACA, 2024–2025 ; FRC, 2025).

Enfin, la gouvernance doit prévoir des boucles d'amélioration : (i) indicateurs (taux de ré-utilisation de scripts validés, incidents évités, couverture populationnelle, temps de cycle, métriques d'équité/robustesse des modèles), (ii) revues indépendantes périodiques (QA interne/qualité externe), (iii) gestion du changement outillée (tests de non-régression, approbations formelles), et (iv) transparence proportionnée envers les parties prenantes (comités d'audit, direction, autorités) sur l'usage et l'impact des outils. Les retours FRC en 2025 montrent que, sans ces mécanismes, l'adoption d'IA reste sous-mesurée, ce qui fragilise la crédibilité des bénéfices revendiqués ; inversement, les fonctions qui combinent cadres + preuves maximisent les gains tout en maîtrisant les risques (FRC, 2025).

### 3.2. Supervision humaine et qualité d'audit

La généralisation des outils d'IA et d'automatisation (RPA) impose de re-centrer la qualité d'audit sur la supervision humaine structurée et sur un régime de preuve documenté. Les Standards mondiaux de l'IIA (2024) rappellent que l'usage d'outils ne transfère ni la responsabilité ni le jugement professionnel : l'auditeur reste tenu à l'intégrité, à l'objectivité, à la diligence et à la traçabilité (Domaine II, *Ethics & Professionalism*). Concrètement, la supervision couvre la conception, l'exécution et la revue des travaux assistés par IA/RPA, avec des pistes d'audit digital (fiches-modèles, journaux d'exécution, documentation des données) reliant les sorties algorithmiques aux assertions et conclusions. Ce recentrage est cohérent avec l'exigence, formulée par les régulateurs, de justifier l'impact réel des outils sur la qualité et non de se limiter au suivi des licences ou du taux d'usage. (IIA, 2024 ; FRC, 2025).

Sur le plan méthodologique, la littérature propose d'opérationnaliser la supervision via un cadre à trois couches distinguant : (1) l'audit de gouvernance (fournisseur/organisation), (2)

l'audit du modèle (avant diffusion), et (3) l'audit d'application (usages dans le contexte d'audit). Cette approche évite de confondre qualité technique du modèle (robustesse, biais, stabilité) et légitimité décisionnelle de son usage dans une mission donnée ; elle aide à assigner clairement les responsabilités et à définir des évidences attendues à chaque niveau (documentation des données, reports d'explicabilité, limites d'emploi, contrôles compensatoires). L'auditeur conserve ainsi la primauté du jugement tout en bénéficiant d'outils plus puissants. (Mökander, et al 2024).

Les enseignements des revues 2025 insistent sur le fait que la plupart des grands cabinets n'évaluent pas encore de façon systématique l'effet des outils d'IA sur la qualité d'audit : ils mesurent l'adoption (comptes, licences, connexions) plutôt que des KPI de performance/éthique (taux de faux positifs/negatifs, impact sur la couverture, rapidité avec garde-fous, explicabilité effective). Les autorités appellent donc à définir des indicateurs formels et des revues indépendantes des cas d'usage, faute de quoi les bénéfices revendiqués restent non démontrés au regard des objectifs de qualité. (FRC, 2025).

Dans cette perspective, la supervision humaine doit être conçue comme un processus qui encadre l'outil avant, pendant et après son usage : *ex ante*, l'auditeur valide l'adéquation du modèle au risque audité (pertinence des données, variables sensibles, équité, matérialité) ; *in itinere*, il contrôle l'exécution (journaux RPA, dérive/instabilité des modèles, seuils d'alerte, tests de sensibilité) ; *ex post*, il revoit l'explicabilité et la cohérence des résultats avec les assertions, ajuste la matérialité et documente le raisonnement professionnel. Les retours d'expérience et travaux empiriques récents montrent que, sans cette supervision "duale" (technique et déontologique), la digitalisation peut déplacer le risque plutôt que le réduire (faux signaux, sur-détection, biais non maîtrisés). (Liang et al., 2025 ; Schiff, 2024).

La gouvernance des automatismes constitue un autre pilier de la qualité. La guidance COSO dédiée à la RPA formalise l'intégration des robots au contrôle interne (objectifs, risques, contrôles, séparation des environnements, journalisation, revue indépendante) : les robots utilisés à des fins d'audit doivent être testés en conception et en efficacité opérationnelle, et accompagnés d'une piste d'audit vérifiable (paramètres, versions, résultats, anomalies traitées). Cette doctrine évite la dépendance opaque à des automatisations "boîte noire" et aligne l'accélération opérationnelle sur une exigence de preuve. (COSO, 2025).

Enfin, la qualité d'audit augmentée par IA/RPA suppose des KPI combinant valeur et garde-fous. Au-delà des métriques de productivité (délai de cycle, couverture populationnelle), la fonction doit suivre des indicateurs d'éthique (équité, explicabilité, confidentialité

opérationnelle) et des mesures d'efficience contrôlée (baisse du taux d'erreurs avec validation humaine). De tels indicateurs, discutés en comité d'audit, créent une redevabilité visible et durable, conforme aux attentes des régulateurs. (FRC, 2025 ; IIA, 2024).

## 4. Éthique et professionnalisme à l'ère digital

### 4.1. Principes éthiques renouvelés

À l'ère des outils d'IA, de RPA et d'analytique avancée, les principes éthiques de l'audit interne demeurent stables dans leur intention (intégrité, objectivité, confidentialité, compétence), mais ils changent d'intensité opérationnelle : l'auditeur doit prouver sa diligence par des évidences digitaux (pistes d'audit, journaux d'exécution, fiches-modèles, documentation des données) et maintenir la primauté du jugement humain dans des environnements sociotechniques complexes (IIA, 2024). Autrement dit, l'éthique n'est plus seulement une posture ; elle devient un dispositif de preuve arrimé à des pratiques de supervision, d'explicabilité et de traçabilité.

Intégrité. Dans les missions assistées par IA/RPA, l'intégrité implique de dire ce que fait réellement l'outil (capabilités, limites, hypothèses), de ne pas sur-vendre sa valeur probante et de signaler les zones d'incertitude liées aux données et aux modèles. Les Standards mondiaux (Domaine II) exigent de documenter l'adéquation entre l'outil et l'objectif de la procédure, ainsi que la séparation des environnements (dev/test/prod) et des responsabilités, afin d'éviter les conflits d'intérêt et les « boîtes noires » non gouvernées (IIA, 2024). Ces exigences rejoignent la guidance COSO sur la RPA, qui formalise objectifs, risques, contrôles, journalisation et revue indépendante des automatismes déployés, y compris lorsqu'ils soutiennent des tests d'audit (COSO, 2025).

Objectivité. L'objectivité est menacée par les biais algorithmiques (sélection d'échantillons, variables proxy), par l'opacité des modèles (LLM, réseaux profonds) et par la sur-confiance aux sorties automatisées. La littérature en *Big Data & Society* montre que les audits d'éthique de l'IA reproduisent les étapes de l'audit financier mais peinent encore sur l'implication des parties prenantes, la mesure du succès et le reporting externe autant de lacunes susceptibles d'affaiblir la crédibilité du jugement (Schiff, 2024). En pratique, l'objectivité se traduit par des tests d'équité, des analyses de sensibilité et une revue indépendante de l'usage de l'IA, distincte de la revue du modèle lui-même.

Confidentialité. L'industrialisation de l'analytique et de la GenAI accroît l'exposition aux fuites, ré-identifications et usages secondaires non autorisés. L'éthique impose de restreindre

les contextes de traitement, d'appliquer pseudonymisation/masquage, de contrôler les flux vers des tiers et de démontrer la licéité des opérations sur la donnée d'audit. Dans la perspective d'un audit « à trois couches » (gouvernance du fournisseur, audit du modèle, audit d'application), l'assurance sur la sécurité et la confidentialité doit être attribuée au bon niveau (fournisseur vs usage interne), avec des évidences alignées (model cards, registres d'accès, rapports d'explicabilité) (Mökander, Schuett, Kirk & Floridi, 2024).

Compétence et diligence professionnelles. Les exigences en compétence ne se limitent plus aux savoirs comptables : elles englobent la littératie des données, l'explicabilité de l'IA, la gouvernance de la qualité (lineage, métriques) et la cybersécurité. Des résultats empiriques (2025) montrent que l'adéquation des talents digitaux réduit le risque de non-détection, tout en révélant un effet médiateur : une digitalisation mal encadrée peut déplacer certains risques (faux positifs, instabilité) si la supervision n'est pas renforcée (Liang et al., 2025). D'où la recommandation d'adosser les compétences à des revues indépendantes et à des KPI d'explicabilité suivis en comité d'audit.

Redevabilité et mesure de l'impact. Les régulateurs rappellent qu'il ne suffit pas d'inventorier les outils : encore faut-il mesurer leur effet sur la qualité d'audit. En 2025, la FRC observe que les grands cabinets suivent surtout les licences et l'usage, mais rarement des KPI de performance/éthique (faux positifs, couverture, délais, explicabilité effective), et les exhorte à instaurer des métriques formelles et des revues documentées (FRC, 2025). Transposé à l'audit interne, ce signal implique de lier les principes éthiques à des indicateurs vérifiables (p. ex. complétude des journaux RPA, score d'explicabilité, incidents de confidentialité évités) et à une boucle d'amélioration continue.

### 4.2. Dilemmes éthiques contemporains

L'essor des outils d'IA (y compris l'IA générative) et de l'automatisation reconfigure la responsabilité de l'auditeur interne en exposant la mission à des biais algorithmiques, à l'opacité décisionnelle et à la dilution de la redevabilité. Les audits d'éthique de l'IA tendent à reproduire les étapes de l'audit financier, mais pêchent encore par une faible implication des parties prenantes, des mesures de succès limitées et un reporting externe lacunaire autant de déficits qui compromettent la crédibilité des dispositifs d'assurance sur l'IA (Schiff, 2024). Ces constats invitent l'auditeur à intégrer, dès la planification, des tests de non-discrimination, des revues indépendantes et des obligations de transparence proportionnées au risque.

Un dilemme central tient au statut de la preuve lorsque les résultats proviennent de modèles opaques (*black box*). L'approche « à trois couches » proposée pour l'audit des LLM gouvernance du fournisseur, audit du modèle, audit de l'application évite la confusion entre qualité technique et légitimité d'usage dans un contexte d'audit donné (Mökander, Schuett, Kirk & Floridi, 2024). Pour l'auditeur interne, la question n'est pas seulement de savoir si le modèle fonctionne, mais s'il est apte à la finalité visée (assertions, matérialité, contexte de risque), avec des évidences traçables (données, hypothèses, limites, contrôles compensatoires).

La confidentialité et la sécurité des données d'audit constituent un autre nœud éthique, particulièrement lorsque des LLM hébergés par des tiers sont utilisés pour la revue documentaire ou l'analyse exploratoire. Un cadre d'assurance d'algorithmes de type criterion audit recommande d'expliciter la portée (données, modèle, processus) et l'evidence (tests adversariaux, métriques quantitatives, entretiens, revues documentaires), en s'inspirant de la chaîne de preuve en audit financier (Lam et al., 2024). En pratique, cela signifie cartographier les flux de données, limiter la sensibilité des corpus, exiger des journalisations et conserver des pistes d'audit exploitables par la qualité interne ou externe.

Le biais de sur-confiance dans l'automatisation constitue un risque méthodologique : l'extension de la couverture (analyses populationnelles, monitoring continu) ne garantit pas la baisse du risque de non-détection si la supervision et l'explicabilité ne suivent pas. Des résultats empiriques montrent que l'adéquation des talents digitaux réduit directement le risque de non-détection, mais que le degré de digitalisation peut jouer un rôle médiateur complexe parfois supprimant une partie du bénéfice attendu si les garde-fous sont insuffisants (OUHOUD, O et al (2025). Liang et al., 2025). Ce paradoxe rappelle que la technologie déplace le cœur du jugement professionnel vers la qualité de la gouvernance des outils (revues indépendantes, métriques d'équité et d'explicabilité).

La redevabilité organisationnelle face aux outils IA reste, elle, incomplètement objectivée. En 2025, le régulateur britannique (FRC) observe que les grands cabinets suivent surtout l'usage (licences, connexions), mais rarement l'impact sur la qualité d'audit (KPI de précision, faux positifs/négatifs, explicabilité effective, couverture) ; il appelle à définir des indicateurs formels et à renforcer la documentation (FRC, 2025). Pour les fonctions d'audit interne, ce signal réglementaire soutient l'adoption d'un tableau de bord éthique (équité, transparence, confidentialité) et d'un plan de revue périodique des cas d'usage.

### 4.3. Mécanismes d'encadrement

Les mécanismes d'encadrement visent à rendre opérationnels les principes éthiques et professionnels de l'audit interne dans des environnements outillés (RPA, IA, data analytics). D'abord, les Global Internal Audit Standards (IIA, 2024) prescrivent une articulation explicite entre compétence, diligence et traçabilité afin que l'usage des technologies reste justifiable et auditable : la fonction doit documenter la supervision humaine, les limites des outils et les preuves qui relient sorties algorithmiques et assertions d'audit (IIA, 2024). L'IIA fournit en outre un outil d'acknowledgement (Domain II) pour formaliser l'adhésion aux exigences « Ethics & Professionalism », utile comme trace de conformité et levier de culture (IIA, 2024).

Ensuite, l'encadrement passe par la gouvernance des automatismes. La guidance COSO sur la RPA (2025) intègre les robots au contrôle interne : définition d'objectifs, évaluation des risques, contrôles, journalisation et revue indépendante. Pour l'audit interne, il s'agit de tester la conception (design) et l'efficacité opérationnelle des automatismes au même titre que des contrôles clés, et de conserver une piste d'audit techniquement vérifiable (paramètres, versions, résultats, anomalies) (COSO, 2025). Cette structuration évite la dépendance à des « boîtes noires » et aligne l'accélération opérationnelle sur un régime de preuve robuste (COSO, 2025).

En matière d'assurance des systèmes algorithmiques, la littérature 2024 propose des cadres auditables. Le "criterion audit" de Lam et al. (ACM FAccT 2024) transpose des pratiques d'audit financier à l'IA en définissant portée, critères et évidence (tests techniques, *adversarial pressure testing*, entretiens, revues documentaires) pour produire une assurance externe ou interne crédible (Lam et al., 2024). De façon complémentaire, l'approche « trois couches » (gouvernance fournisseur, audit du modèle, audit d'application) guide la séparation des responsabilités et le choix des preuves (données, explicabilité, limites d'usage), évitant de confondre qualité technique et légitimité décisionnelle (Mökander et al., 2024).

Le développement des compétences et la supervision sont des mécanismes transverses. Le Global Practice Guide - Internal Auditing Competency Framework (IIA, 2025) propose des gabarits pour cartographier les compétences par rôle, fixer des niveaux de maîtrise et relier la montée en compétences aux exigences des Standards (plans, évaluations, preuves) (IIA, 2025). Cette approche outille la redevabilité des équipes et soutient la baisse du risque de non-détection lorsque les talents digitaux sont au rendez-vous et supervisés de façon appropriée (Liang et al., 2025).

Enfin, les indicateurs de maturité assurent la mesure et la transparence de l'encadrement. Le régulateur britannique FRC (2025) appelle les professionnels à dépasser le seul suivi des licences/usages pour instrumenter des KPI d'impact (précision, faux positifs/négatifs, couverture, délais, explicabilité effective) et documenter le raisonnement qui relie l'outil à la qualité d'audit (FRC, 2025). Pour l'audit interne, ces attentes se traduisent par des tableaux de bord qualité/éthique, des revues indépendantes périodiques et des politiques précisant les seuils d'acceptabilité (par exemple score d'explicabilité minimal, complétude des journaux) (Reda, K. et al 2026).(FRC, 2025).

**Conclusion générale**

Ce travail a montré que l'auditeur interne de l'ère digital est un professionnel hybride, à l'intersection de la technicité digitale (data analytics, RPA, IA/GenAI, cybersécurité) et de la déontologie (intégrité, objectivité, confidentialité, diligence). Les Global Internal Audit Standards (édition 2024) consacrent cette double exigence en réaffirmant la primauté du jugement humain, la traçabilité des travaux et l'obligation de preuve (evidence) lorsque des outils digitaux sont mobilisés ; l'usage de la technologie ne transfère ni la responsabilité ni le jugement du professionnel. Autrement dit, la transformation digitale n'abolit pas les principes de la profession : elle en rehausse l'intensité opérationnelle en exigeant que chaque résultat outillé soit rattaché à des éléments probants et à une supervision explicite.

Sur le plan empirique, les résultats récents indiquent que la maturité des talents digitaux réduit le risque de non-détection et accroît la pertinence des missions, à condition que la digitalisation s'accompagne d'un pilotage par la qualité (revues indépendantes, explicabilité mesurée, indicateurs d'équité) (Liang et al., 2025). Inversement, une adoption opportuniste de scripts et de modèles peut déplacer les risques (sur-détection, faux positifs, opacité), rappelant que la valeur de l'audit augmenté se situe moins dans l'outil que dans la gouvernance de son usage et la capacité critique de l'équipe (Liang et al., 2025 ; Vitali & Giuliani, 2024). Cette lecture rejoint les constats des pratiques professionnelles : la promesse d'un audit plus étendu, rapide et traçable est réelle, mais elle requiert une re-planification des jalons (données en amont, explicabilité et validation humaine en aval) ainsi qu'un investissement soutenu dans l'acculturation et la formation continue.

Normativement, un alignement de cadres renforce la robustesse du dispositif : COSO pour l'intégration des automatismes au contrôle interne (objectifs, risques, contrôles, journalisation, revues indépendantes), COBIT/ISACA pour la gouvernance SI (rôles, decision

rights, gestion du changement), et IIA 2024 pour la responsabilité professionnelle et l'éthique ; à cela s'ajoute l'exigence croissante des régulateurs de mesurer l'impact effectif des outils sur la qualité d'audit par des KPI formels (FRC, 2025 ; COSO, 2025 ; IIA, 2024). En parallèle, la littérature sur l'audit de l'IA propose des architectures d'assurance cadre « trois couches » (gouvernance du fournisseur, audit du modèle, audit d'application) qui clarifient les responsabilités et évitent de confondre qualité technique et légitimité décisionnelle (Mökander, Schuett, Kirk & Floridi, 2024). (Mökander et al., 2024 ; COSO, 2025 ; FRC, 2025)

Au total, la contribution de cet article est double. Théoriquement, il articule une matrice techno-éthique des compétences où la maîtrise des outils (IA, RPA, data, cybersécurité) est inséparable de vertus professionnelles opérationnalisées (intégrité = transparence d'usage ; objectivité = tests d'équité et revues indépendantes ; confidentialité = gouvernance des données ; diligence = explicabilité et supervision) (IIA, 2024 ; Mökander et al., 2024). Pratiquement, il fournit des pistes d'implémentation : cartographies de compétences par rôle, checklists d'encadrement, KPI combinant valeur et garde-fous, et un régime de preuve reliant systématiquement sorties algorithmiques, assertions d'audit et matérialité. Pour les contextes émergents (dont le Maroc), des études longitudinales et quasi-expérimentations sont encouragées afin d'évaluer l'effet des trajectoires d'upskilling et des politiques d'explicabilité sur la qualité et la confiance (FRC, 2025 ; Liang et al., 2025 ; Vitali & Giuliani, 2024). L'auditeur interne qui réussit cette transition demeure, in fine, le gardien du sens il sait interroger les algorithmes, documenter le raisonnement et rendre compte conditions sine qua non d'une assurance crédible dans l'économie digital.

## BIBLIOGRAPHIE

1. Al Frijat, Y. S., & Al-Hajaia, E. M. (2025). *Auditor's technical, digital, and creativity skills and their role in supporting audit outcomes in light of digital transformation strategy*. *Corporate Board: Role, Duties and Composition*, 21(1), 60–70.
2. Chen, Y., Zhao, H., & Wang, J. (2024). *Data privacy challenges in the digital audit environment: Insights from practitioners*. Journal of Information Systems, 38(1), 37–52.
3. Cheong, B. C., et al. (2024). *Transparency and accountability in AI systems*. Frontiers in Human Dynamics.
4. COSO (2025). Achieving Effective Internal Control Over Robotic Process Automation (gouvernance RPA, ICIF).
5. COSO / The CPA Journal. (2025). *COSO Issues Guidance on Robotic Process Automation* (gouvernance de la RPA et contrôle interne).
6. De Araujo, P. G. L. (2025). *Adoption of emerging technologies in a regulated context: Factors influencing digital transformation in auditing*.
7. Deloitte. (2025) How WestRock harnessed GenAI to enhance Internal Audit (adoption sécurisée, formation incrémentale, supervision humaine).
8. Deloitte. (2025). *Global internal audit hot topics 2025: Risks and opportunities* (GenAI, cybersécurité, fraude, talents).
9. EY. (2025). *Déploiement d'outils IA pour l'audit et l'assurance* (presse économique).
10. Fang, Q., et al. (2025). Audit effort in the digital era: Uncovering the dynamic effects of business strategy and digitalization. *International Journal of Accounting Information Systems*.
11. Financial Reporting Council (FRC). (2025). *AI in audit: review & guidance* (vérifier l'impact qualité, définir des KPI). Presse & trade press :
12. Financial Times. (2025). *Big accounting firms fail to track AI impact on audit quality, says regulator* (synthèse des constats FRC).
13. Hossain, S. (2025). *The Impact of Emerging Technology on the Role of Auditors in Reshaping the Future of Audit*. *European Journal of Accounting, Auditing and Finance Research*, 13(4), 37–58.
14. 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.
15. 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
16. 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).
17. 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.
18. 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).

19. IIA Ethics & Professionalism (Domain II) (2024). *Global Internal Audit Standards™* (pour cadrage déontologique général).
20. IIA Research Foundation (2024). *Solving the Riddle: Harnessing Generative AI for Internal Audit Activities* (rapport de recherche, méthodologie d'enquête et gouvernance).
21. IIA. (2024–2025). *Ethics & Professionalism : Overview/Tool* (applicabilité, exigences, formulaire d'acknowledgement
22. IIA. (2024–2025). *Page d'orientation et mappages 2017 ↔ 2024* (Standards Two-Way Mapping; Glossary Comparison; effectivité 9 janv. 2025).
23. ISACA. (2024). *Unlocking AI's Potential: How COBIT Can Guide Your Business Transformation* (blog cadrant l'usage de COBIT pour l'IA).
24. ISACA. (2025). *Leveraging COBIT for Effective AI System Governance* (white paper).
25. Kamar, R. E. D. A., & JAMAL, A. (2024). Exploration du Rôle des Outils Technologiques dans l'Optimisation de la Gestion des Ressources Humaines dans le secteur Hôtelier Marocain. *Economics and Management Review*, *2*(2).
26. Kamar, R., & Abdelfattah, J. (2025, April). Bibliometric Analysis of Scientific Trends Around the Key Concepts of the New Era: Digital Transformation and Human Resources Management. In *International Conference on Digital Technologies and Applications* (pp. 233-245). Cham: Springer Nature Switzerland.
27. Kokina, J., et al. (2025). *Challenges and opportunities for artificial intelligence in auditing*. International Journal of Accounting Information Systems.
28. KPMG. (2024–2025). *Internal audit insights 2025 / Transformation & Technology* (agilité, priorités, compétences).
29. Lam, K., et al. (2024). *A Framework for Assurance Audits of Algorithmic Systems*. ACM FAccT 2024.
30. Liang, L., Dai, T., Cui, L., & Song, M. (2025). *Digital audit talent's impact on audit digitization and detection risk*, Scientific Reports.
31. Mökander, J., Schuett, J., Kirk, H. R., & Floridi, L. (2023). *Auditing large language models: a three-layered approach*..
32. OUHOUD, O., & EL OUAFA, K. (2025). Le rôle transformationnel de l'intelligence artificielle dans l'audit interne à l'ère du digital. *International Journal of Accounting Finance Auditing Management and Economics*, *6*(10), 560-578.
33. OUHOUD, O., & EL OUAFA, K. (2025). Transformation digitale et audit financier: Réflexions sur les risques et leurs dispositifs de gestion. *Revue du contrôle, de la comptabilité et de l'audit*, *9*(3).
34. PwC. (2024). *Global Workforce Hopes and Fears Survey 2024* (upskilling et GenAI).
35. Reda, K., Jamal, A., & Benraïss, B. (2026). A Systematic Review of Employees' Behavior in Adopting Innovative Technologies: Aligning AI and Digital Transformation Projects. *AI, Transparency, and Organizational Change*, 1-48.
36. Sayal, A., et al. (2025). *Optimizing audit processes through open innovation*. *ScienceDirect*.
37. Schiff, D. S. (2024). *The emergence of artificial intelligence ethics auditing*. Big Data & Society.

38. The Institute of Internal Auditors (IIA). (2024). *Global Internal Audit Standards™* Domain II: Ethics & Professionalism 9 janv. 2025
39. The Institute of Internal Auditors (IIA). (2025). Global Practice Guide: Internal Auditing Competency Framework™. (PDF officiel).
40. The Institute of Internal Auditors (IIA). (2025). *The Catalyst for Strong AI Governance* (Global Best Practices).
41. Vitali, S., & Giuliani, M. (2024). *Emerging digital technologies and auditing firms: Opportunities and challenges*. *International Journal of Accounting Information Systems*, 53, Article 100676.
42. Zweers, B., Dey, D., & Bhaumik, D. (2025). *The AI-Fraud Diamond: A Novel Lens for Auditing Algorithmic Deception*.