Revue du Contrôle de la Comptabilité et de l'Audit
ISSN: 2550-469X
Volume 9 : numéro 3

Transformation digitale et audit financier : Réflexions sur les risques et leurs dispositifs de gestion

Digital transformation and financial auditing: Reflections on risks and their management mechanisms

OUHOUD Omar
Doctorant en Sciences de Gestion,
Université Cadi Ayyad-Maroc
Laboratoire : Innovations, Responsabilités et Développement Durable (INREDD)

EL OUAFA Khalid
Enseignant Chercheur,
Université Cadi Ayyad-Maroc
Laboratoire : Innovations, Responsabilités et Développement Durable (INREDD)

Date de soumission : 04/08/2025
Date d'acceptation : 11/10/2025
Pour citer cet article :
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 « Volume 9 : numéro 3 /:» pp : 239 – 265
Digital Object Identifier : https://doi.org/10.5281/zenodo.17561450

Résumé :

Cet article propose une revue exploratoire à dominante conceptuelle sur l'impact de la transformation digitale sur l'audit financier, en mettant l'accent sur l'évaluation et la gestion des risques. Nous structurons les constats en trois familles : risques liés aux données (qualité, lignée, biais), risques de sécurité/confidentialité/conformité (cybersécurité, IAM, RGPD/AI) et risques comportement/compétences (lacunes digitales, scepticisme professionnel, gouvernance de l'IA). La méthodologie s'appuie sur une revue narrative structurée complétée couvrant revues à comité de lecture et référentiels professionnels Nous proposons un cadre intégrateur reliant technologies ; profils de risques ; réponses d'audit (procédures, éléments probants, documentation) et traduisons ces liens en outils opérationnels (matrices de traitement, check-lists données/cyber, KPI de pilotage et surveillance continue). Les résultats soulignent la primauté de la data quality et de la posture cyber, la nécessité d'upskilling ciblé et l'importance d'une explicabilité des modèles pour préserver la qualité du jugement. L'article se conclut par des recommandations pour la planification des missions et des pistes de recherche appliquée

Mots clés : Transformations digitale - Audit financier - Risques - Gestion Efficace - Digitalisation

Abstract :

This article presents an exploratory, concept-driven review of the impact of digital transformation on financial auditing, with a focus on risk assessment and risk management. We organize the evidence into three families: data-related risks (quality, lineage, bias); security, privacy, and compliance risks (cybersecurity, IAM, GDPR/AI Act); and behavioral/skills risks (digital skills gaps, professional skepticism, AI governance). The methodology relies on a structured narrative review of peer-reviewed literature complemented by professional frameworks. We propose an integrative framework that links technologies to risk profiles and to audit responses (procedures, audit evidence, documentation), and translate these links into operational tools (risk-treatment matrices, data/cyber checklists, KPI-based steering, and continuous monitoring). The findings highlight the primacy of data quality and cyber posture, the need for targeted upskilling, and the importance of model explainability to preserve the quality of professional judgment. The article concludes with practice-oriented recommendations for engagement planning and avenues for applied research.

Keywords : Digital Transformation - Financial Audit - Risks - Effective Management - Digitalization

Introduction

La transformation digitale est un phénomène d'actualité qui suscite aujourd'hui un vif intérêt parmi les chercheurs et les professionnels. Ce concept englobe les changements profonds et omniprésents, tant dans la société que dans les industries, rendus possibles par les technologies digitales (Majchrzak et al., 2016). Dans le domaine de l'audit, la digitalisation a démontré son efficacité en optimisant les processus d'évaluation, permettant une réduction des risques dans les audits des entreprises publiques comme privées. Elle améliore ainsi la qualité et la rapidité des audits grâce à des méthodes d'analyse avancée de données et à une automatisation accrue des processus (Zhang & Balia, 2024).

L'audit demeure un élément central de la gouvernance organisationnelle, garantissant la transparence et la fiabilité des informations financières. Ce rôle est d'autant plus crucial dans un environnement économique marqué par une complexité croissante et par des innovations technologiques rapides. En tant que pilier de confiance, l'audit protège les intérêts des parties prenantes, incluant investisseurs, créanciers et consommateurs. Toutefois, le développement accéléré des technologies présente à la profession d'audit des défis inédits, redéfinissant de manière significative ses pratiques et son champ d'action.

Dans ce sens, l'étude de Wu, Zhao et Su (2025) souligne que la transformation digitale influence non seulement la qualité des informations d'audit, mais aussi la manière dont les auditeurs formulent et présentent les « key audit matters » dans leurs rapports.

La digitalisation se traduit par l'intégration des technologies digitales dans les processus d'affaires, redéfinissant en profondeur les méthodes de travail des auditeurs. Des technologies telles que l'intelligence artificielle (IA), l'analyse de données massives (big data), la blockchain et l'automatisation des processus facilitent les audits en permettant des analyses plus précises et en réduisant les risques d'erreurs humaines. Par exemple, l'IA peut aider à détecter rapidement des anomalies dans les transactions financières, rendant les audits non seulement plus rapides, mais aussi plus fiables (AICPA, 2022). En complément, Zhang (2025) rappelle que la blockchain constitue désormais un champ d'expérimentation majeur pour l'audit, en raison de ses capacités de traçabilité et d'automatisation des contrôles via les smart contracts. Cependant, cette transformation digitale s'accompagne également de nouveaux risques. Les auditeurs font face à des enjeux croissants en matière de cybersécurité, de protection des données, et se doivent de développer des compétences techniques avancées pour appréhender ce nouvel environnement technologique (KPMG, 2023). Les travaux de Liang (2025) mettent en évidence que le manque de talents digitaux accroît le risque de

détection insuffisante, ce qui souligne l'importance d'une montée en compétences des auditeurs

Les impacts de la digitalisation sur le risque d'audit sont ainsi ambivalents : d'un côté, les outils technologiques renforcent la qualité et l'efficacité des audits, mais de l'autre, ils exposent les entreprises et leurs auditeurs à des risques accrus, tels que ceux liés à la sécurité des systèmes d'information, à la confidentialité des données et à la maîtrise des compétences techniques nécessaires. Par exemple, les cyberattaques ou les violations de données peuvent entraîner des pertes financières significatives et ternir la réputation des organisations (Deloitte, 2024).

Pour faire face à ces défis, il est essentiel que les auditeurs adoptent une approche proactive dans l'évaluation et la gestion des risques. Cela implique la mise en place de systèmes de gestion des risques digitaux robustes, une formation continue des professionnels de l'audit, ainsi que l'intégration des meilleures pratiques en matière de sécurité et de gestion de l'information. Une étude de l'International Federation of Accountants (IFAC, 2023) souligne que les auditeurs investissant dans des formations sur les technologies émergentes et les méthodes de gestion des risques sont mieux armés pour relever les défis liés à la digitalisation. Des travaux soulignent également que la transformation digitale reconfigure les profils de risques et appelle des dispositifs de gouvernance adaptés (EL YAMANI, K et al, 2023). Ces constats rejoignent des travaux récents sur le rôle transformationnel de l'IA dans l'audit, qui détaillent à la fois les apports (couverture, détection) et les risques méthodologiques (explicabilité, supervision humaine) associés. *(*Ouhoud & El Ouafa*, 2025)*.

Au regard de ce qui a été présenté, la question sous-jacente de notre travail de recherche alors est de savoir « **Comment les professionnels de l'audit peuvent-ils adapter leurs méthodes et pratiques pour assurer une évaluation fiable et pertinente des risques dans un environnement de plus en plus digitalisé ?** »

Cette problématique pourrait être subdivisée en trois sous-questions suivantes :

- **Quels sont les risques potentiels liés au comportement et aux compétences des employés dans le contexte de la digitalisation et comment peuvent-ils être évalués et gérés de manière efficace ?**
- **Comment l'évaluation et la gestion des risques peuvent-elles être appliquées pour minimiser les risques liés à la sécurité, à la confidentialité et à la conformité dans un environnement digital en constante évolution ?**

- **Quels sont les principaux risques liés aux données dans le cadre de la digitalisation et quelles mesures peuvent être prises pour assurer leur protection et leur intégrité lors des audits ?**

Cet article adopte une démarche exploratoire à dominante conceptuelle, s'appuyant sur une revue narrative structurée de la littérature académique et professionnelle relative aux effets de la transformation digitale sur l'audit financier. L'objectif est de confronter les cadres classiques de l'audit par les risques et les référentiels ISA aux nouveaux paradigmes induits par les technologies intelligentes. Le protocole de revue couvre la période 2019-2025 et mobilise les bases (Scopus, Web of Science, ScienceDirect/Elsevier, Wiley, SpringerLink…) ainsi que des sources professionnelles (IAASB, IIA, ISACA, IAPP, CSA, …).

Les critères d'inclusion requièrent : un ancrage audit & risques, une qualité de source (pairs/organismes de référence), un lien explicite avec les procédures d'audit (identification/évaluation des risques, réponses, éléments probants). Ce positionnement hybride, à la fois théorique et pratique, vise moins à produire une généralisation qu'à éclairer les tensions, limites et opportunités de l'audit en contexte digital (qualité des données, cybersécurité, conformité/explicabilité, compétences). Après avoir présenté le cadre conceptuel, l'article analyse les effets de l'intégration des technologies sur le profil de risques et les procédures d'audit, discute les enjeux éthiques et organisationnels (gouvernance algorithmique, supervision humaine) et propose enfin des recommandations opérationnelles.

1. Cadre conceptuel

1.1. Concept de l'audit

L'audit constitue un processus structuré et systématique qui permet d'évaluer de manière objective les états financiers, les processus ou les opérations d'une organisation, afin de vérifier leur conformité, leur exactitude et leur fiabilité (Arens, Elder, & Beasley, 2020). Historiquement, l'audit financier s'est principalement concentré sur la vérification des états financiers, assurant ainsi une transparence accrue pour les parties prenantes, notamment les investisseurs et les régulateurs. L'objectif fondamental de l'audit est de fournir une assurance raisonnable aux parties prenantes quant à la véracité et la conformité des informations financières, ce qui contribue à réduire les asymétries d'information (Louwers et al., 2018).

Le processus d'audit s'appuie sur un cadre théorique bien défini, qui inclut notamment les concepts d'indépendance et de matérialité. L'indépendance de l'auditeur est essentielle pour

garantir l'objectivité de l'audit, condition qui est particulièrement encadrée par des normes éthiques établies par des organismes comme l'International Ethics Standards Board for Accountants (IESBA). En 2025, le Code of Ethics de l'ICAEW a été mis à jour pour renforcer les dispositions relatives à l'indépendance, en particulier pour le rôle de l'Engagement Quality Reviewer (EQR) dans les audits des entités à forte influence publique (ICAEW, 2025) En ce qui concerne la matérialité, ce concept est crucial pour évaluer l'impact d'une erreur ou d'une omission significative sur les états financiers (Power, 2019).

L'audit moderne est régi par des normes internationales, telles que les Normes internationales d'audit (ISA), qui fournissent des directives précises tout au long du processus d'audit. Édictées par l'International Federation of Accountants (IFAC), ces normes reposent sur une approche axée sur les risques, signifiant que l'auditeur doit évaluer et identifier les zones de risque dans les états financiers et adapter ses procédures en conséquence (Johnstone et al., 2019). Des recherches montrent que, dans l'ère de la digitalisation, les auditeurs doivent aussi intégrer la dimension technologique du risque dans leurs plans d'audit (Fang, 2025), ce qui recompose le périmètre des contrôles traditionnels.

Du point de vue théorique, plusieurs modèles soutiennent la fonction et l'importance de l'audit. La théorie de l'agence, formulée par Jensen et Meckling (1976), présente l'audit comme un instrument destiné à limiter les conflits d'intérêts entre actionnaires (principaux) et dirigeants (agents). L'audit réduit les asymétries d'information, renforçant la confiance des investisseurs. La théorie de la signalisation (Spence, 1973) complète ce cadre : un audit de haute qualité signale aux parties prenantes que l'entreprise adhère à des standards stricts de gouvernance, ce qui rehausse sa crédibilité sur les marchés. Plus récemment, Visedsun et al. (2025) ont étendu l'application de ces théories en étudiant comment la qualité d'audit (issue de méthodes modernes) renforce la relation entre les résultats comptables et la valeur de marché de l'entreprise, confirmant que l'audit joue à la fois un rôle d'agence et de signal vers les investisseurs.

1.2 Concept de la digitalisation

La digitalisation, souvent désignée sous le terme de « transformation digitale », fait référence au processus d'intégration des technologies digitale dans tous les aspects des opérations d'une organisation. Cette transformation impacte profondément les processus internes, les relations avec les clients et les partenaires, ainsi que le modèle d'affaires (Rogers, 2016). La digitalisation s'appuie sur des technologies clés telles que le cloud computing, l'intelligence artificielle et les Big Data, permettant aux entreprises d'optimiser leur productivité et de créer

de nouveaux canaux de distribution et de communication (Bharadwaj et al., 2013). L'adoption combinée de l'IA, du cloud sécurisé et de l'analytique avancée influence fortement la maturité digitale des organisations (Guo, 2024).

Cette digitalisation a également des répercussions théoriques significatives sur la gestion et l'organisation. Le cadre des capacités dynamiques (Teece, 2018) est fréquemment utilisé pour décrire comment les entreprises acquièrent, intègrent et reconfigurent leurs compétences pour faire face aux transformations technologiques. Selon cette approche, les entreprises capables d'adapter rapidement leurs ressources et processus aux évolutions Digitale sont mieux placées pour maintenir un avantage concurrentiel sur le marché.

Parallèlement, la théorie de la contingence soutient que l'efficacité des pratiques organisationnelles dépend du contexte dans lequel elles sont appliquées (Woodward, 1965). Dans le contexte de la digitalisation, cette théorie indique que chaque entreprise doit ajuster sa stratégie digitale en fonction de ses caractéristiques spécifiques, telles que sa taille, son secteur d'activité et ses objectifs stratégiques (Vial, 2019). Récemment, Liang (2025) a confirmé que les stratégies digitales optimales varient selon la dimension sectorielle, la disposition technologique et les infrastructures disponibles.

D'autre recherches révèlent également que la digitalisation transforme les modes de gouvernance d'entreprise en introduisant de nouveaux risques liés à la cybersécurité et à la protection des données, nécessitant des ajustements dans les structures de contrôle et de gestion des risques (Sebastian et al., 2017). Ainsi, elle impose aux entreprises une approche plus agile et réactive pour faire face à l'incertitude croissante de l'environnement technologique. Guo (2025) met en avant que l'intégration de la blockchain dans les processus d'entreprise exige une reconfiguration des contrôles internes et des garanties de traçabilité.

1.3 Concept du risque

Le risque est généralement défini comme l'incertitude concernant les événements futurs susceptibles d'influencer l'atteinte des objectifs d'une organisation (Rejda & McNamara, 2017). Dans le monde des affaires, le risque se présente sous plusieurs formes, notamment les risques financiers, opérationnels, de marché et technologiques. Chaque type de risque nécessite une évaluation approfondie et une stratégie de gestion spécifique afin de minimiser ses impacts potentiellement négatifs.

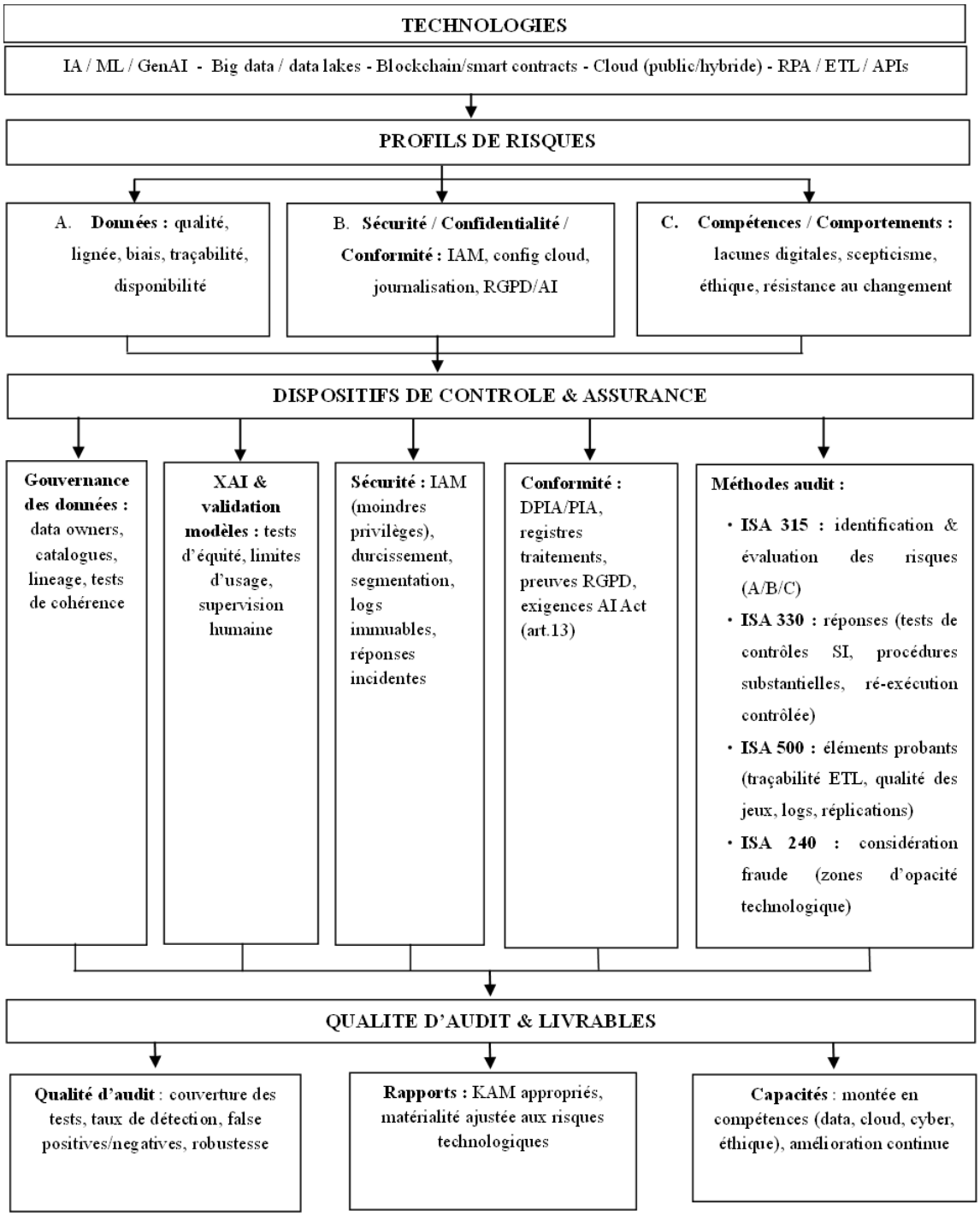
Parmi les théories les plus influentes en matière de gestion des risques, le modèle de gestion des risques COSO (Committee of Sponsoring Organizations of the Treadway Commission) propose un cadre intégré pour identifier, évaluer et gérer les risques. Ce modèle repose sur des

principes de contrôle interne visant à assurer raisonnablement l'atteinte des objectifs stratégiques, opérationnels, de reporting et de conformité (COSO, 2017). La mise en œuvre de ce cadre aide les entreprises à intégrer la gestion des risques dans leur processus décisionnel, favorisant ainsi une approche proactive face aux incertitudes (Frigo & Anderson, 2011). Des travaux récents suggèrent la nécessité de l'intégrer avec les risques technologiques, (Liang, 2025).

De plus, la théorie de la diversification des risques, introduite par Markowitz (1952), constitue un fondement essentiel de la gestion des risques financiers. Cette théorie suggère qu'il est possible de réduire le risque global d'un portefeuille d'investissements en répartissant stratégiquement les actifs. Elle repose sur le principe que des actifs non corrélés permettent de diminuer l'impact des fluctuations individuelles, optimisant ainsi la performance du portefeuille sans accroître significativement le risque (Elton et al., 2014).

La digitalisation complexifie davantage la notion de risque en introduisant de nouvelles menaces cybernétiques. Ainsi, la gestion des risques doit inclure une évaluation continue de la sécurité des systèmes d'information, ainsi que de la confidentialité et de l'intégrité des données (Singer & Friedman, 2014). Face à ces évolutions, la théorie de la gestion agile des risques devient de plus en plus pertinente, préconisant une approche flexible et adaptative pour réagir rapidement aux risques émergents et imprévus (Kate, B. Clive,T. 2024). L'adoption de l'analytique prédictive des risques via modèles d'apprentissage automatique est proposée comme méthode émergente pour anticiper les scénarios de risque digital (Fang, 2025).

Figure 1 : Cadre intégrateur « Technologies, Risques, Contrôles/Assurance, Qualité d'audit »



Sources : Zhang et al. (2022) Han et al. (2023) KPMG (2024 ; EY–IIF (2025) Cloud Security Alliance (2024); IAPP & EY (2024); IIA (2025); PCAOB (2025)

2. Effets de la digitalisation sur le risque d'audit

La digitalisation reconfigure le profil de risque de l'audit en conjuguant gains d'efficacité et nouvelles expositions. L'IA et l'analyse de données renforcent la couverture des tests et la détection d'anomalies, mais exigent des dispositifs d'explicabilité et une traçabilité de la preuve d'audit compatibles avec les standards professionnels (Zhang et al., 2022). De même, la blockchain et les architectures cloud soutiennent l'intégrité et la disponibilité des informations, tout en introduisant des risques de gouvernance des données et de dépendance aux tiers qui requièrent des contrôles adaptés (Han et al., 2023).

Les risques liés aux données deviennent centraux. Les fonctions finance/audit rapportent que la qualité des données est un levier critique et un risque prioritaire, 66% des dirigeants placent la data quality au premier plan de la mitigation des risques IA (KPMG, 2024), tandis que les CRO bancaires classent la qualité/provenance des données comme risque n°1 d'usage des données (EY–IIF, 2025). Ces constats imposent des contrôles renforcés sur la préparation des données (gouvernance, lignée, biais) et l'adéquation des jeux de données aux objectifs d'audit.

L'exposition cyber s'intensifie avec la concentration de données sensibles et l'interconnexion des chaînes applicatives. Les directions d'audit classent de façon récurrente la cybersécurité en tête des risques (IIA, 2025). Dans les environnements hybrides/multicloud, la mauvaise configuration et une gestion IAM insuffisante figurent parmi les menaces majeures, ce qui justifie des contrôles d'accès et de change management stricts (CSA, 2024). Ces tendances confirment la nécessité d'outiller et former les auditeurs aux aspects SI/cyber (ISACA, 2024) et de maintenir une gouvernance de la sécurité à l'échelle de l'audit.

Les compétences constituent un facteur déterminant. Les pénuries de profils cyber et les lacunes de compétences observées par ISACA (2024) militent pour des plans d'upskilling et une intégration méthodique des outils digitaux dans la méthodologie d'audit. Les modèles récents d'audit « co-piloté » par l'IA suggèrent des gains de productivité/qualité lorsque l'IA assiste l'auditeur tout en respectant des garde-fous de gouvernance, de sécurité et d'éthique (Gu et al., 2024).

Enfin, l'approche prédictive et continue qu'autorisent les données en temps réel doit rester équilibrée par le jugement professionnel. Les positions de l'IAASB (International Auditing and Assurance Standards Board) rappellent que la technologie améliore la qualité mais ne remplace pas le scepticisme professionnel ; côté régulateur, le PCAOB (Public Company Accounting Oversight Board) alerte sur les risques de sur-dépendance à l'automatisation qui

peuvent affaiblir la supervision humaine et la qualité du jugement. Les équipes doivent donc articuler analytics/IA et revues manuelles de manière complémentaire.

2.1 Risques liés aux données

Avec l'adoption croissante de technologies digitales pour la collecte et l'analyse des données, les risques associés deviennent une préoccupation majeure pour les auditeurs. Ils affectent la qualité des audits, la fiabilité des rapports financiers et la conformité aux réglementations.

L'un des risques majeurs concerne la qualité. La dépendance à des systèmes automatisés de collecte et de transformation (ETL- Extract, Transform, Load, API - Application Programming Interface, IA) expose les audits à des problèmes d'exactitude, d'exhaustivité et de traçabilité susceptibles d'altérer les conclusions. Les enquêtes récentes placent la data quality au premier rang des priorités de mitigation des risques technologiques 66% des dirigeants la citent comme axe central lors des déploiements d'IA (KPMG, 2024), dans la banque, la qualité et la provenance des données demeurent un déterminant principal des priorités de gestion des risques (EY & IIF, 2025). En pratique, cela impose des contrôles robustes gouvernance et lignée des données, validations en amont, tests de cohérence et journalisation des transformations. Par ailleurs, Guo (2024) rapporte que même une faible proportion d'enregistrements erronés peut biaiser des analyses prédictives.

Les algorithmes d'analyse peuvent hériter ou amplifier des biais historiques, influençant la sélection des transactions, le scoring d'anomalies ou la hiérarchisation des tests. La littérature récente en audit assisté par IA souligne la nécessité d'une gouvernance des données, de tests d'équité et d'une supervision humaine effective pour prévenir les discriminations involontaires et préserver la qualité du jugement (Murikah, 2024 ; Zhang et al., 2022).

Dans un contexte de digitalisation et de chaînes applicatives interconnectées, la menace s'intensifie selon le Thales Data Threat Report 2024, 49 % des organisations déclarent avoir déjà subi une violation (et 14 % au cours de la dernière année). Dans les environnements hybrides/multicloud, les contrôles d'identité/accès (IAM Identity and Access Management) et la maîtrise des configurations/changements demeurent des points critiques à auditer, figurant parmi les principales menaces recensées par la Cloud Security Alliance (2024). Les plans d'audit doivent donc couvrir à la fois la prévention (segmentation, moindres privilèges, durcissement, journalisation) et la réponse aux incidents (détection, notification, remédiation).

Au-delà de la sécurité, l'obligation de conformité renforce les exigences de documentation, de traçabilité et de transparence. L'IAPP (2024) montre qu'une part significative d'organisations ne mène pas d'évaluations de risques privacy régulières (23 % n'en font pas, 25 % seulement

déclenchées à l'occasion d'événements), révélant un déficit de revues/audits systématiques. En parallèle, l'AI Act (UE, 2024) introduit des obligations de transparence par exemple l'article 13 pour les systèmes à haut risque concernant l'information sur les limites, les conditions d'usage, les performances et les risques, ainsi que la documentation nécessaire à l'interprétation et à la réutilisation contrôlée des modèles.

La maîtrise des risques données requiert un cadre intégré combinant qualité & traçabilité des jeux de données, atténuation des biais par tests d'équité et supervision humaine, posture de sécurité adaptée aux architectures hybrides/multicloud, et conformité continue (privacy-by-design, exigences AI Act). Cette articulation soutient la fiabilité de la preuve d'audit et la conformité réglementaire, tout en réduisant les risques de conclusions erronées.

2.2 Risques liés à la sécurité, à la confidentialité et à la conformité

La digitalisation des processus d'audit renforce l'exposition aux menaces à mesure que les entreprises adoptent des systèmes digitaux de stockage et de traitement, la surface d'attaque s'élargit. Des constats récents font état d'une augmentation des cyberattaques, faisant de la cybersécurité une priorité pour les auditeurs (Peters et al., 2023). Il est dès lors essentiel d'évaluer la robustesse des contrôles (prévention, détection, réponse), y compris l'apport d'outils de détection proactive et d'IA de cybersécurité, qui peuvent réduire le risque de compromission (Fang, 2025).

La confidentialité s'impose comme un enjeu central les auditeurs doivent garantir la conformité des traitements sur tout le cycle de vie des données (collecte, usage, archivage) et démontrer la traçabilité des contrôles. Les enquêtes internationales montrent l'ampleur des difficultés de mise en conformité (IAPP-EY, 2024). Parallèlement, le niveau des sanctions en Europe (plus de 2 200 amendes totalisant plus de 5,6 Mds €) illustre la pression réglementaire (CMS, 2025). Dans ce contexte, les procédures d'audit doivent intégrer la vérification du RGPD et la montée en puissance des exigences de l'AI Act (Zhao, 2025).

Au-delà des volets sécurité et privacy, le risque de non-conformité aux normes financières et d'audit demeure. Les auditeurs doivent s'assurer que les systèmes d'information respectent les exigences applicables (collecte, stockage, traitement, contrôles). Les environnements fortement digitalisés dépourvus de procédures claires peuvent générer des zones d'opacité propices à la fraude (Guo, 2024).

L'essor de l'IA et des analytiques soulève des questions de responsabilité lorsque des algorithmes soutiennent les jugements d'audit, l'attribution des responsabilités en cas d'erreur se complexifie (concepteurs, déployeurs, équipes d'audit). La littérature recommande une

gouvernance explicite documentation des modèles et des données, traçabilité des décisions, supervision humaine effective et auditabilité (tests d'équité, revues indépendantes) pour établir des lignes de responsabilité claires (Munoko et al., 2020; Mökander et al., 2023). À cela s'ajoute la nécessité d'explicabilité (XAI) pour maintenir la confiance des parties prenantes et préserver l'indépendance professionnelle (Liang, 2025).

1.2.3 Risques liés au comportement et aux compétences

La transition digitale transforme le profil de compétences attendu des auditeurs (data, IA, cloud), tout en réaffirmant le rôle du jugement professionnel *(*Lahsini & Taouab, 2024*)*. Ces évolutions requièrent un upskilling ciblé (data/IA) et un maintien du scepticisme professionnel face aux systèmes automatisés (Ouhoud & El Ouafa, 2025). La digitalisation de l'audit requiert non seulement des outils technologiques avancés, mais également des compétences comportementales et techniques appropriées. Tout d'abord, les lacunes en compétences digitales constituent un risque majeur. L'évolution des systèmes (data analytics, IA, cybersécurité, cloud, blockchain) impose aux auditeurs des savoirs et savoir-faire nouveaux depuis la gouvernance des données jusqu'aux contrôles technologiques. Les enquêtes professionnelles récentes confirment un déficit de compétences les employeurs signalent des gaps significatifs, notamment en soft skills (51 %) et en compétences cloud (42 %), qui compliquent l'évaluation de dispositifs digitaux complexes (ISACA, 2024). Les diagnostics de la profession (Pulse of Internal Audit) appellent donc à un développement professionnel continu et à l'intégration d'outils/compétences digitaux dans la méthodologie d'audit (IIA, 2024/2025). Les travaux de (Vitali, 2024) montrent par ailleurs que l'IA/RPA reconfigure les processus d'audit, ce qui renforce l'exigence de nouvelles compétences pour maintenir la qualité et la robustesse des conclusions. Selon Zhao (2025), l'absence de compétences digitales spécialisées accroît significativement le risque de détection insuffisante des anomalies.

En outre, les attitudes et comportements des auditeurs conditionnent la qualité des audits. Un ancrage éthique solide intégrité, scepticisme professionnel, sens des responsabilités réduit le risque de jugements biaisés ou de décisions discutables. La littérature montre que les conflits éthiques vécus par les auditeurs, ainsi que la perception de défaillances éthiques au sein de la profession, influencent concrètement leurs comportements et, in fine, la qualité des audits (Tormo-Carbó et al., 2024). Parallèlement, l'usage croissant d'outils digitaux et d'algorithmes accroît le risque de sur-dépendance technologique, des travaux soulignent la nécessité de

maintenir un scepticisme actif et des contre-vérifications humaines afin d'éviter des erreurs de jugement (Van Liempd et al., 2025).

Enfin, les recherches sur l'éthique de l'IA appliquée à l'audit identifient des biais et des risques de responsabilité qui appellent des dispositifs robustes de gouvernance des modèles, de traçabilité et de supervision humaine (Murikah, 2024). Dans ce contexte, les cabinets doivent promouvoir une culture d'intégrité et intégrer des formations régulières à l'éthique pour atténuer ces risques. Fang (2025) souligne que l'intégrité digitale, incluant la capacité à résister aux pressions liées à l'automatisation des décisions, devient une compétence centrale.

Par ailleurs, la résistance au changement demeure un frein comportemental majeur. Certains auditeurs préfèrent des méthodes éprouvées et manifestent une réticence à adopter de nouveaux outils ou approches, ce qui peut ralentir l'innovation et réduire l'efficacité des missions. Les enquêtes confirment que les facteurs culturels pèsent significativement dans la réussite des transformations l'ACCA classe « *employee resistance to adoption* » parmi les premiers obstacles à l'implémentation technologique au sein des fonctions finance ou audit, soulignant l'importance d'un accompagnement du changement structuré (communication, formation, leadership). De son côté, l'Internal Audit Foundation (IIA) montre que des mindsets hérités et des lacunes de compétences freinent l'innovation, d'où la nécessité d'une acculturation et d'un développement professionnel continu pour ancrer durablement les nouvelles pratiques. Guo (2024) met en avant que cette résistance soit particulièrement forte dans les environnements organisationnels où la digitalisation est perçue comme une menace pour l'autonomie professionnelle. Il est crucial d'encourager une mentalité ouverte au changement pour surmonter ce défi.

Enfin, le bien-être mental et émotionnel des auditeurs est un déterminant de la qualité d'audit. Les délais serrés, la pression d'exigences élevées et l'accélération digitale peuvent accroître la charge cognitive et la fatigue décisionnelle. Les enquêtes internationales de l'ACCA indiquent que plus d'un professionnel sur deux (55 %) rapporte une dégradation de sa santé mentale liée au travail, tendance accentuée par les transformations technologiques et les modèles de travail hybrides (ACCA, 2024). Sur le plan académique, des travaux montrent que les dimensions de stress (ambiguïté/surcharge de rôle, contraintes temporelles) sont associées à une baisse de la qualité des audits, via des effets sur l'attention, le scepticisme professionnel et la persévérance dans les tests (IFAC, 2023). Ces constats plaident pour des dispositifs de prévention (planification réaliste des missions, ressources adaptées, rotations), une culture managériale bienveillante, ainsi que des programmes de formation au repérage du stress et à

l'hygiène mentale (ex : charge de travail soutenable, récupération, accès à des soutiens dédiés). Liang (2025) précise que l'intensification du travail digital et la surveillance algorithmique peuvent engendrer une fatigue cognitive accrue, nécessitant la mise en place de dispositifs de soutien psychologique et de programmes de résilience.

3. Évaluation et gestion des risques

L'évaluation et la gestion des risques sont des processus essentiels dans l'audit contemporain, surtout à l'ère de la digitalisation. Alors que les organisations intègrent des technologies avancées pour améliorer leur efficacité, elles se heurtent également à des risques nouveaux et complexes qui nécessitent une attention particulière. Dans cette section, nous examinerons les différentes étapes de l'évaluation et de la gestion des risques, ainsi que les meilleures pratiques adoptées par les professionnels de l'audit.

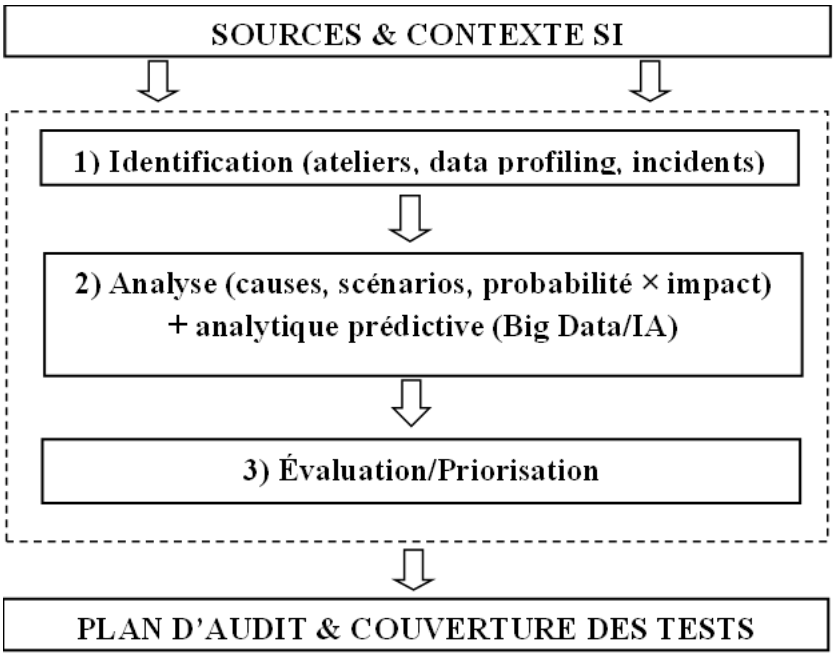
3.1 Processus d'évaluation des risques

L'évaluation des risques est un processus systématique visant à identifier, analyser et évaluer les risques susceptibles d'affecter les objectifs d'une organisation. Dans le contexte de l'audit, cela implique de comprendre les divers types de risques, notamment opérationnels, financiers, de conformité et stratégiques. Ce processus comprend plusieurs étapes clés :

- **Identification des risques** : Cette étape consiste à repérer les menaces potentielles pouvant impacter l'organisation. Les auditeurs doivent collaborer avec les parties prenantes pour obtenir une vision complète des risques auxquels l'entreprise est confrontée. Une étude de Peng, Y., & Jin, H. (2025) soulignent que l'audit moderne requiert des diagnostics partagés pour couvrir les risques émergents dans les systèmes d'information. Selon (Alotaibi, 2023), l'intégration de l'analyse prédictive basée sur le Big Data permet d'anticiper les zones de vulnérabilité avant l'émergence des signes évidents.
- **Analyse des risques** : Une fois les risques identifiés, ils doivent être analysés pour comprendre leur nature, leur origine et leur impact potentiel. Les auditeurs peuvent recourir à des outils quantitatifs et qualitatifs pour évaluer la probabilité de survenue de chaque risque et son impact sur l'organisation. Peng & Jin (2025) montre que l'application de l'informatique et des technologies de l'information dans les audits influence positivement le niveau de gestion du risque d'entreprise, démontrant l'efficacité des techniques analytiques avancées (Peng et al., 2025).

- **Évaluation des risques** : Après l'analyse, les auditeurs doivent évaluer les risques en les classant selon leur niveau de gravité. Cela permet de prioriser les risques en fonction de leur potentiel d'impact. Les risques critiques nécessitent une attention immédiate, tandis que les risques moins significatifs peuvent être surveillés. **Lombardi et al. (2025)** notent que les technologies avancées notamment les plateformes d'analyse prédictive facilitent l'évaluation dynamique des risques, en ajustant les priorités à mesure que les données évoluent.

Figure 1 : Chaîne d'évaluation du risque



Sources : Peng & Jin (2025) ; Alotaibi (2023) ; Lombardi et al. (2025).

3.2 Gestion des risques

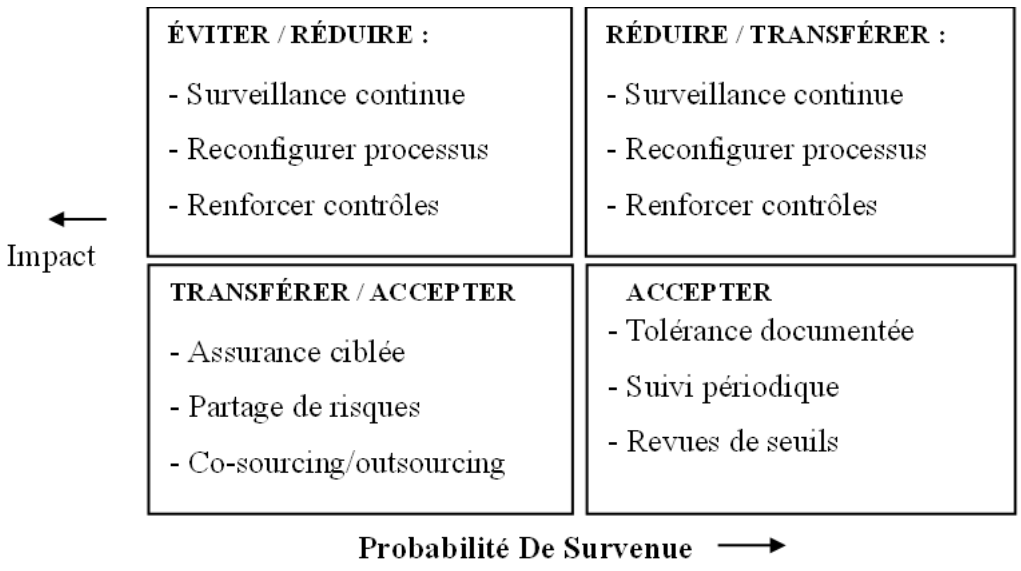
La gestion des risques est le processus par lequel une organisation élabore des stratégies pour atténuer les risques identifiés. Cela implique de prendre des décisions éclairées sur la manière de gérer chaque risque en fonction de son niveau de gravité. Les principales stratégies de gestion des risques comprennent :

- Évitement du risque : Dans certains cas, une organisation peut choisir d'éviter un risque en modifiant ses activités. Par exemple, si un risque élevé est identifié dans le cadre d'un nouveau projet, l'entreprise peut décider de ne pas s'engager dans cette initiative. Dans les audits financiers modernisés, cela peut signifier l'exclusion de

certaines missions à haut risque non maîtrisables technologiquement sans renforcement préalable du contrôle (Risk in Focus 2025).

- Réduction du risque : Cette approche vise à minimiser la probabilité ou l'impact d'un risque en instaurant des contrôles internes et des mesures préventives. Les audits internes sont cruciaux à cette étape, car ils permettent de détecter les faiblesses des systèmes de contrôle et de recommander des améliorations. Selon l'étude de Wang (2025), cette réduction des risques s'accompagne d'une amélioration de la valeur d'entreprise quand la qualité de l'audit est élevée
- Transfert du risque : Une organisation peut choisir de transférer un risque à un tiers, par exemple, en souscrivant une assurance pour couvrir les pertes potentielles dues à une cyberattaque. Dans le cadre de la digitalisation, ce transfert peut également passer par la délégation de contrôles technologiques à des fournisseurs certifiés (gestion externalisée).
- Acceptation du risque : Dans certaines situations, une organisation peut décider d'accepter un risque, surtout si le coût des mesures d'atténuation dépasse les pertes potentielles. Cette approche nécessite une surveillance continue pour s'assurer que le risque demeure dans des limites acceptables. La nouvelle version des normes IIA (2025) insiste sur la mise en place de seuils de tolérance au risque documentés et revus périodiquement (IIA 2025)

Figure 2. Matrice de traitement du risque (éviter, réduire, transférer, accepter).



Sources : IIA (2025) ; Risk in Focus (2025) ; Wang (2025).

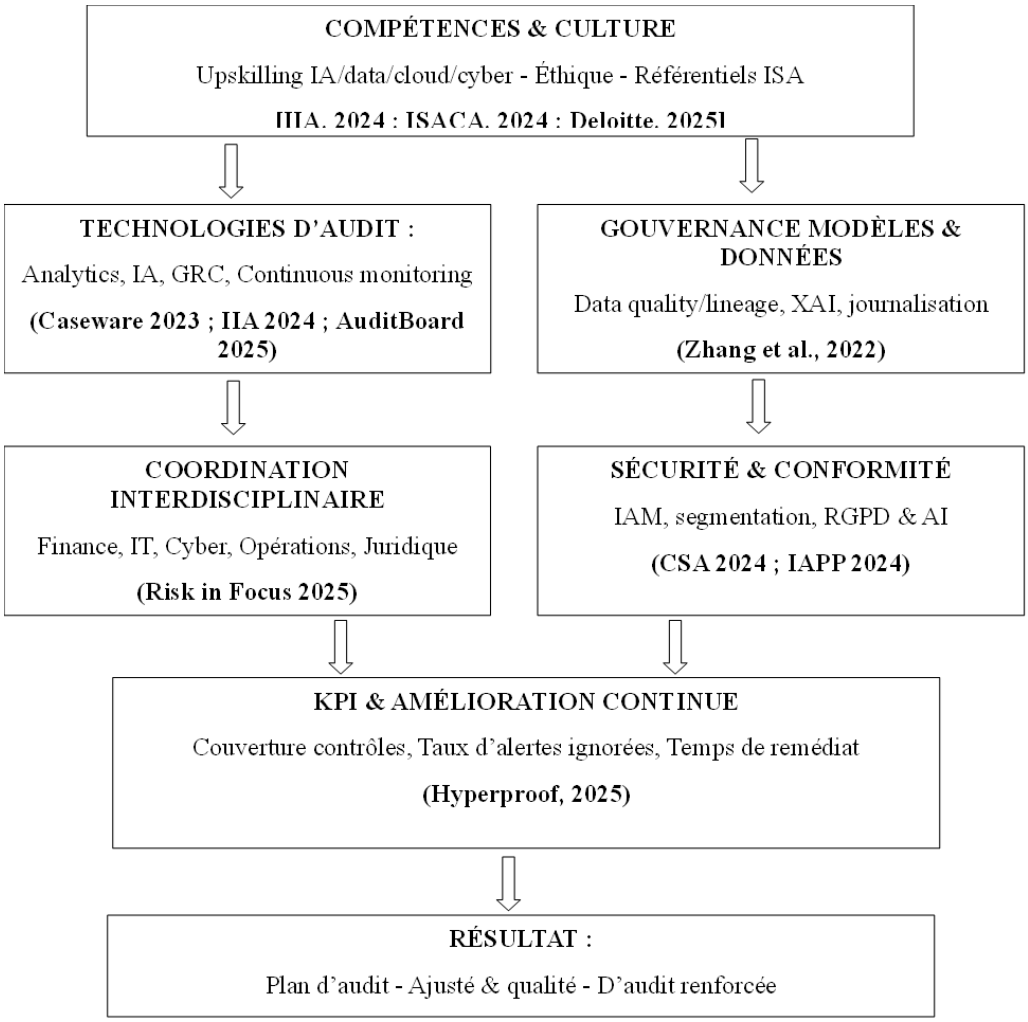
3.3 Meilleures pratiques en matière d'évaluation et de gestion des risques

Pour garantir une évaluation et une gestion efficaces des risques, les auditeurs doivent adopter certaines meilleures pratiques :

- Formation continue : Les auditeurs doivent suivre des formations régulières pour rester informés des évolutions réglementaires, technologiques et des meilleures pratiques en gestion des risques. Les Global Internal Audit Standards (IIA, 2024) imposent explicitement le développement professionnel continu afin de garantir la maîtrise des référentiels, des méthodes de cartographie et des contrôles liés aux technologies émergentes. Parallèlement, les enquêtes ISACA (2024) mettent en évidence des lacunes de compétences notamment sur les dimensions cyber et cloud qui justifient des programmes d'upskilling ciblés. Dans cette logique, Deloitte (2025) classe la GenAI et la cybersécurité parmi les thématiques prioritaires pour l'audit interne, ce qui plaide pour des plans de formation incluant des modules dédiés (IA, cybersécurité, éthique et gouvernance des données)
- Collaboration interdisciplinaire : La gestion des risques nécessite une approche collaborative impliquant différentes parties prenantes, y compris les équipes financières, opérationnelles et informatiques. Les auditeurs doivent établir des canaux de communication clairs pour favoriser cette collaboration. L'approche « risk in focus » 2025 préconise d'impliquer les équipes de TI, de cyber-sécurité et des opérations dans la co-construction des programmes de contrôle.
- Utilisation de technologies avancées : Les outils d'analyse de données, l'intelligence artificielle et les plateformes de gestion des risques permettent d'identifier plus tôt les signaux faibles et d'objectiver l'évaluation des risques. Côté adoption, des enquêtes récentes indiquent que l'analytics est déjà une composante clé pour 56 % des équipes d'audit, tandis que 34 % supplémentaires prévoient de l'intégrer à court terme ; l'usage de l'IA générative progresse également au niveau des organisations (65 % déclarent l'utiliser régulièrement), ce qui accélère la disponibilité d'outils au service des missions d'audit (Caseware, 2023 ; IIA, 2024). Ces apports exigent toutefois des dispositifs de gouvernance des modèles et des données afin d'assurer l'explicabilité, la qualité des jeux de données et la traçabilité des preuves, De plus, l'adoption de la surveillance continue (continuous risk monitoring) devient une pratique de référence, permettant de détecter les signaux faibles en temps réel (AuditBoard, 2025)

- Mise en place de métriques de performance : Les organisations doivent établir des indicateurs de performance pour suivre l'efficacité de leurs efforts en gestion des risques, permettant ainsi d'ajuster les stratégies selon les résultats obtenus. La pratique moderne consiste à intégrer des indicateurs tels que le temps de détection des risques, le nombre de contrôles exécutés, le taux d'alertes ignorées, etc. (Hyperproof, 2025).

Figure 3. Cadre d'outillage et de pilotage (compétences-technologies-KPI).



Sources : IIA (2024) ; ISACA (2024) ; Deloitte (2025) ; Caseware (2023) ; AuditBoard (2025) ; Zhang et al. (2022) ; CSA (2024) ; IAPP (2024) ; Hyperproof (2025).

L'évaluation et la gestion des risques sont des éléments essentiels du processus d'audit moderne, particulièrement dans un environnement de plus en plus digitalisé. Les auditeurs doivent être proactifs dans l'identification et la gestion des risques, en adoptant des approches systématiques et en intégrant des technologies avancées. En adoptant des pratiques

exemplaires, les professionnels de l'audit peuvent garantir la qualité et la fiabilité des audits, tout en contribuant à la pérennité et à la croissance des organisations.

Conclusion

En conclusion, la digitalisation transforme radicalement la profession d'auditeur, apportant des avantages considérables tout en soulevant de nouveaux défis. Les technologies Digitale offrent des opportunités pour améliorer l'efficacité et la précision des audits, mais elles introduisent également des risques complexes qui nécessitent une gestion attentive. L'évolution rapide des technologies impose aux auditeurs d'adopter une approche proactive et adaptative en matière d'évaluation et de gestion des risques.

L'évaluation et la gestion des risques sont des éléments fondamentaux pour garantir la qualité des audits dans un contexte de digitalisation. En adoptant des pratiques exemplaires telles que la formation continue, la collaboration interdisciplinaire et l'utilisation d'outils technologiques avancés, les professionnels de l'audit peuvent mieux anticiper et atténuer les risques associés à cette transformation (ACCA, 2023).

De plus, il est essentiel que les auditeurs favorisent un environnement de travail propice à l'innovation, à l'intégrité et à l'éthique. Cela inclut la promotion d'une culture organisationnelle qui valorise la transparence, la responsabilité et le bien-être mental des employés (IFAC, 2023). Les résultats d'une étude de McKinsey (2023) révèlent que les firmes d'audit qui investissent dans le bien-être et la formation de leurs équipes affichent de meilleures performances et réagissent plus efficacement aux défis technologiques.

Dans cette ère de changements rapides, les auditeurs doivent demeurer vigilants, adaptables et engagés envers l'amélioration continue. Une compréhension approfondie des enjeux liés à la digitalisation et des risques associés est cruciale pour assurer l'efficacité et la pertinence de la profession d'auditeur dans les années à venir. En intégrant ces réflexions dans leurs pratiques, les auditeurs peuvent non seulement relever les défis posés par la digitalisation, mais aussi en tirer parti pour renforcer la confiance des parties prenantes et contribuer à la durabilité des organisations

Références

1) Adams, R., & Smith, L. (2023). Compliance gaps in financial audit systems. *Journal of Financial Regulation*.
2) Arens, A. A., Elder, R. J., & Beasley, M. S. (2020). *Auditing and assurance services: An integrated approach* (16e éd.). Pearson.
3) Association of Chartered Certified Accountants (ACCA). (2023). *Digital horizons: Technology, innovation, and the future of accounting.* ACCA. Association of Chartered Certified Accountants (ACCA). (2023). *Navigating the digital landscape: The future of audit in a digital age.* ACCA.
4) AuditBoard. (2025). *Solidifying risk management: How to get started with continuous monitoring.* AuditBoard. https://auditboard.com/blog/solidifying-risk-management-how-to-get-started-with-continuous-monitoring
5) Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly, 37*(2), 471–482. https://doi.org/10.25300/MISQ/2013/37:2.3
6) Chen, Y., et al. (2024). Data privacy and audit practice: Challenges in a digital environment. *Accounting Horizons*.
7) Cloud Security Alliance. (2024). *Top threats to cloud computing 2024.* Cloud Security Alliance.
8) CMS Law. (2025). *GDPR Enforcement Tracker – Numbers and figures / Statistics.* CMS.
9) Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise risk management: Integrating with strategy and performance.* COSO.
10) Davis, J., & Lee, H. (2023). Digital resistance in audit practices: A behavioral analysis. *Journal of Accounting Research*.
11) Dounia, G. A. G. A., KAIZAR, C., AGOUDAL, A., BENARBI, H., & HILMI, Y. (2025). Transformation digitale et mutation du métier de contrôleur de gestion: revue de littérature et perspectives. Revue Française d'Economie et de Gestion, 6(3).
12) Deloitte. (2023). *Global future of cyber survey* (4e éd.). Deloitte.
13) Deloitte. (2024). *Risk management in a digital world: Best practices for auditors.* Deloitte Insights.

14) Deloitte. (2025). *Internal audit hot topics 2025: Risks and opportunities.* Deloitte. https://www.deloitte.com/us/en/services/audit-assurance/articles/internal-audit-hot-topics-2025-risks-and-opportunities.html

15) El Yamani, K., Kasbaoui, T., & Ait Larbi, F. E. (2023). De la transformation digitale responsable et inclusive : enjeux, risques et perspectives. *Revue Internationale des Sciences de Gestion, 6*(2). https://www.revue-isg.com/index.php/home/article/view/1332

16) Elton, E. J., Gruber, M. J., Brown, S. J., & Goetzmann, W. N. (2014). *Modern portfolio theory and investment analysis* (9e éd.). Wiley.

17) EY & Institute of International Finance (IIF). (2025). *14th annual global bank risk management survey.* EY.

18) Fang, Q. (2025). Audit effort in the digital era: Uncovering the dynamic impact of digitalization and strategy. *International Journal of Accounting Information Systems*. https://www.sciencedirect.com/science/article/pii/S1467089525000235

19) Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting & Finance, 22*(3), 81–88.

20) Garcia, M., & Lopez, J. (2022). Ethical issues of algorithmic auditing. *Journal of Business Ethics*.

21) Gu, H., et al. (2024). Artificial intelligence co-piloted auditing. *International Journal of Accounting Information Systems*.

22) Guo, R. (2024). The effect of audit digital transformation on audit quality. *Journal of Emerging Technologies in Accounting*. https://www.tandfonline.com/doi/full/10.1080/21697213.2024.2442769

23) Guo, X. (2025). A study on applying blockchain smart contracts in auditing. *Journal of Accounting Information Systems*. https://www.sciencedirect.com/science/article/abs/pii/S1467089525000065

24) Han, H., et al. (2023). Accounting and auditing with blockchain technology and AI: A literature review. *International Journal of Accounting Information Systems, 48*.

25) IAASB. (2024). *Technology position statement: 8 actions to embrace technology and innovation.* International Auditing and Assurance Standards Board.

26) IAPP & EY. (2024). *Privacy governance report 2024.* International Association of Privacy Professionals.

27) ICAEW. (2025). *2025 code of ethics and auditor independence.* Institute of Chartered Accountants in England and Wales. https://www.icaew.com/insights/viewpoints-on-the-news/2025/jun-2025/2025-code-of-ethics-and-auditor-independence

28) IFAC. (2023). *Supporting auditor competence in a digital era.* International Federation of Accountants.

29) Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360.

30) Johnstone, K. M., Gramling, A. A., & Rittenberg, L. E. (2019). *Auditing: A risk-based approach to conducting a quality audit* (11e éd.). Cengage Learning.

31) Journal of Accountancy. (2024). Data analytics and visualization in the audit. Journal of Accountancy.

32) HILMI, Y., & KAIZAR, C. (2023). Le contrôle de gestion à l'ère des nouvelles technologies et de la transformation digitale. Revue Française d'Economie et de Gestion, 4(4).

33) 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.

34) 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

35) 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).

36) 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.

37) 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).

38) 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).

39) 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).

40) Hilmi, Y. (2014). Degré d'intégration de l'audit interne et performance des entreprises marocaines/cas de la région de rabat-sale-Zemmour-Zaïr.

41) Kate, B. Clive,T. (2024). *Fundamentals of risk management* (7th ed.). https://www.koganpage.com/risk-compliance/fundamentals-of-risk-management-9781398618657?

42) Kezazy, H. E., & Hilmi, Y. (2025). Promoting the Energy Transition Throughout Dealing with the Climate Change Issue. In Digital Technology for an Innovative Energy Transition: Perspectives and Opportunities (pp. 77-93). Cham: Springer Nature Switzerland.

43) KPMG. (2023). *Audit 2023: Adapting to the new reality of digital risks.* KPMG.

44) Kumar, S., & Patel, R. (2022). Stress and adaptation in digital audit environments. *International Journal of Auditing*.

45) Lahsini, H., & Taouab, O. (2024). Adapting to the digital era: Transformations in the audit profession and the emergence of new skills. *Revue Internationale des Sciences de Gestion, 7*(1), 882–897.

46) Lee, C., Kim, D., & Park, H. (2023). Compliance audits in the age of data protection: Trends and challenges. *International Journal of Accounting Information Systems, 50*, 1–15.

47) Liang, L. (2025). Digital audit talent's impact on audit digitization and detection risk. *Preprint*. https://pmc.ncbi.nlm.nih.gov/articles/PMC12378205/

48) Lombardi, D. R., et al. (2025). The increased role of advanced technology and expert predictions for audit support. *International Journal of Accounting Information Systems*. https://doi.org/10.1016/j.accinf.2025.100733

49) Louwers, T. J., Ramsay, R. J., Sinason, D. H., Strawser, J. R., & Thibodeau, J. C. (2018). *Auditing and assurance services* (6e éd.). McGraw-Hill.

50) Markowitz, H. (1952). Portfolio selection. *The Journal of Finance, 7*(1), 77–91.

51) McKinsey & Company. (2023). *Thriving in the digital age: Strategies for auditors and their firms.* McKinsey.

52) Miller, D., & Thompson, G. (2023). Skill gaps in digital auditing. *Journal of Accounting Education*.

53) Mökander, J., et al. (2023). Auditing of AI: Legal, ethical and technical approaches. *Digital Society*.

54) Munoko, I., Brown-Liburd, H., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics, 167*(2), 209–234.

55) Murikah, W. (2024). Bias and ethics of AI systems applied in auditing. *Journal of Accounting Literature*.

56) PCAOB. (2025). *Conversations with audit committee chairs – Spotlight.* Public Company Accounting Oversight Board.

57) Peng, Y., & Jin, H. (2025). Effects of information and technology application in audits and digital economy on enterprise risk management level. *Finance Research Letters, 73*, 106593. https://doi.org/10.1016/j.frl.2024.106593

58) Peters, A., et al. (2023). Cyber risk management in audit firms. *Journal of Information Security*.

59) Peters, A., Johnson, M., & Wang, L. (2023). Cybersecurity risks in the audit profession: Current trends and future directions. *Journal of Accounting and Public Policy, 42*(5), 1–18.

60) Power, M. (2019). *The audit society: Rituals of verification* (2e éd.). Oxford University Press.

61) Rejda, G. E., & McNamara, M. J. (2017). *Principles of risk management and insurance* (13e éd.). Pearson.

62) Rogers, D. L. (2016). *The digital transformation playbook: Rethink your business for the digital age.* Columbia University Press.

63) Sebastian, I. M., Ross, J. W., Beath, C. M., Mocker, M., Moloney, K. G., & Fonstad, N. O. (2017). How big old companies navigate digital transformation. *MIS Quarterly Executive, 16*(3), 197–213.

64) Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

65) Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics, 87*(3), 355–374.

66) Teece, D. J. (2018). Dynamic capabilities as (workable) management systems theory. *Journal of Management & Organization, 24*(3), 359–368.

67) Thales. (2024). *Data threat report 2024.* Thales.

68) The Institute of Internal Auditors (IIA). (2024). *Global internal audit standards™.* The IIA.

69) The Institute of Internal Auditors (IIA). (2025). *GTAG 3: Continuous auditing* (2e éd.). The IIA. https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/gtag-3-continuous-auditing/gtag-3-continuous-auditing-2nd-edition.pdf

70) The Institute of Internal Auditors (IIA). (2025). *Risk in Focus 2025: Global report.* The IIA Research Foundation.

71) The Institute of Internal Auditors (IIA). (2025). *Risk in Focus 2025: North America.* The IIA Research Foundation. https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2025/2025-na-report-en-riskinfocus.pdf

72) Tormo-Carbó, G., et al. (2024). Should I stay or should I go? Auditor ethical conflict and […]. *Journal of Business Ethics*.

73) Van Liempd, D., Theis, J. C., & Sutton, S. G. (2025). The risk of technology dominance in using digital decision aids in assurance engagements: Evidence from a survey among Danish auditors. *Accounting Horizons, 39*(3), 175–194.

74) Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems, 28*(2), 118–144.

75) Visedsun, N., et al. (2025). Does audit quality enhance the value relevance of earnings and book value? *Journal of Risk and Financial Management, 18*(10), 547.

76) Vitali, S. (2024). Emerging digital technologies and auditing firms. *International Journal of Accounting Information Systems*. https://www.sciencedirect.com/science/article/pii/S1467089524000095

77) Wang, P. (2025). Enhancement of audit quality and optimization of risk management. *Journal of Business Research.*

78) Woodward, J. (1965). *Industrial organization: Theory and practice.* Oxford University Press.

79) Wu, W., Zhao, Y., & Su, Z. (2025). A study on the impact of digital transformation on auditor decision-making. *FBEM Journal.* https://drpress.org/ojs/index.php/fbem/article/view/29750

80) Zhang, C. A., et al. (2022). Explainable AI in auditing. *International Journal of Accounting Information Systems, 45*.

81) Zhang, L., & Balia, S. S. (2024). Digital transformation and corporate audit risk: Mediating effects of auditor behavior. *Finance Research Letters, 67*, 105754. https://doi.org/10.1016/j.frl.2024.105754

82) Zhang, Y. (2025). Auditing in the blockchain: A literature review. *Frontiers in Blockchain.*https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2025.1549729/pdf

83) Zhao, T. (2025). Auditors' digital expertise and audit quality. *Journal of Accounting, Auditing & Finance.*

84) 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.

85) KPMG. (2024, août). *GenAI survey 2024 – Key insights* (data quality = 66 %).

86) Règlement (UE) 2024/1689. (2024, 12 juillet). *Artificial Intelligence Act* (art. 13 – Transparence). *Journal officiel de l'Union européenne.*

87) AICPA. (2022, 20 juillet). *Implementing the new audit evidence standard (SAS No. 142).* American Institute of CPAs.

88) Internal Audit Foundation (The IIA). (2024, 23 septembre). *Demystifying AI: Internal audit use cases for applying new technology.* Internal Audit Foundation. Internal Audit Foundation (The IIA). (2024–2025). *Pulse of internal audit* (rapports).

89) Caseware. (2023, 23 octobre). *Using data analytics to improve audit quality* (State of Internal Audit Trends 2023).