https://www.rag.sn/
Revue électronique internationale
ISSN 2712-7133

Influence des mécanismes de contrôle sur le risque de fraude en contexte dématérialisé : une analyse empirique dans l'administration fiscale au Bénin

Georges AGOSSA[1], Judith Monique Baï GLIDJA[2]

Reçu le : 04 février 2025 ***Accepté le : 07 mai 2025*** ***Mise en ligne le : 15 septembre 2025***

Mots clés:
Risque de fraude
Mcanismes de contrôle
Dématérialisation
Administration fiscale

RÉSUMÉ

Cette étude analyse l'influence des mécanismes de contrôle sur le risque de fraude dans l'administration fiscale béninoise en contexte de dématérialisation. Elle adopte une méthodologie mixte: 15 entretiens semi-structurés et une enquête menée auprès de 305 agents. Trois mécanismes sont examinés: le contrôle d'accès informatique, le contrôle de conformité automatisé et la séparation des tâches. L'analyse qualitative confirme leur pertinence perçue, mais seule l'analyse quantitative du contrôle d'accès révèle un effet modéré et significatif. Les résultats soulignent la nécessité d'assurer une cohérence entre outils technologiques, organisation et contexte pour renforcer l'efficacité de la lutte contre la fraude.

Adresse de correspondance des auteurs :
1. hierag@yahoo.fr
2. judithglid@yahoo.fr

INTRODUCTION

La fraude fiscale demeure l'un des principaux obstacles à la mobilisation efficiente des ressources publiques, limitant de manière significative la capacité des États à financer leurs politiques économiques et sociales. Comme le souligne l'OCDE, « la fraude érode la base d'imposition et affaiblit la confiance dans les institutions fiscales » (OCDE, 2023, p. 14). Cette problématique s'avère particulièrement aiguë en Afrique subsaharienne, où l'assiette fiscale reste étroite et où les administrations fiscales sont confrontées à de multiples contraintes structurelles : systèmes de collecte peu performants, insuffisance de personnel qualifié, prépondérance du secteur informel et faiblesse des outils de traçabilité (Fjeldstad et Moore, 2008 ; Moore, Prichard et Fjeldstad, 2018).

Dans un tel contexte, les capacités de détection et de prévention de la fraude demeurent limitées, notamment parce que les dispositifs traditionnels de contrôle apparaissent inadaptés à la complexité croissante des pratiques frauduleuses. Au Bénin, les rapports de la Cour des comptes (2019, 2021) et de l'Inspection générale des finances (IGF, 2020) ont révélé de nombreuses failles dans le système de contrôle fiscal, en particulier en matière de TVA et de fiscalité foncière. Ces insuffisances traduisent une gouvernance fiscale réactive, marquée par des vérifications a posteriori peu systématiques et faiblement outillées pour prévenir les fraudes en amont.

Deux perspectives théoriques permettent d'éclairer ces constats. D'une part, l'approche structurelle met en exergue les défaillances institutionnelles, le faible niveau de redevabilité et la fragilité des infrastructures numériques (Tazi, 2022 ; Albee, Hesse et Tetteh, 2021). D'autre part, l'approche comportementale insiste sur l'influence des perceptions d'iniquité fiscale, du déficit de légitimité des prélèvements et de la méfiance institutionnelle dans les comportements de fraude (Kirchler, 2007 ; Torgler, 2011). Le modèle du « triangle de la fraude » proposé par Cressey demeure, à cet égard, une référence fondatrice pour l'analyse des comportements frauduleux. Ce modèle postule que « la fraude survient lorsque trois conditions sont réunies : la pression, l'opportunité et la rationalisation » (Cressey, 1953, p. 31). Toutefois, conçu dans un contexte analogique, il montre aujourd'hui ses limites face aux mutations induites par la transformation numérique des processus fiscaux.

Par ailleurs, si la digitalisation promet une amélioration de la traçabilité et une réduction des marges de manœuvre des fraudeurs, elle introduit également de nouveaux risques : piratage de données, manipulation des systèmes d'information, contournement des algorithmes de vérification (Gupta, 2021 ; Flowerday et Tuyikeze, 2016). Néanmoins, certaines expériences récentes en Afrique illustrent les effets positifs de la modernisation numérique sur l'efficacité fiscale. Au Rwanda, par exemple, la mise en œuvre de l'e-Tax et de la facturation électronique a permis « une amélioration significative de la mobilisation des recettes fiscales » (Rwanda Revenue Authority, 2020, p. 7 ; FMI, 2021, p. 25). Le Sénégal et l'Éthiopie ont également engagé des réformes similaires, fondées sur l'interopérabilité des bases de données et l'automatisation des contrôles (Banque mondiale, 2022, p. 19).

Le Bénin, quant à lui, a entamé en 2010 un processus de dématérialisation de son administration fiscale, à travers l'implémentation de la plateforme eSINTAX, suivie plus récemment de la facture normalisée (DGI, 2022, p. 3). Ces innovations visent à élargir l'assiette fiscale, à faciliter le suivi des transactions et à renforcer la conformité. Toutefois, leur mise en œuvre rencontre des défis importants : coût élevé des équipements, déficit de formation technique et résistances organisationnelles (OCDE, 2021, p. 17 ; id., 2023, p. 14).

Ainsi, la modernisation technologique ne saurait, à elle seule, garantir l'efficacité des dispositifs antifraude. Comme le soulignent Mikes et Kaplan, « l'efficacité du contrôle dépend de sa capacité à articuler rigoureusement l'automatisation, la gouvernance de l'information et la structuration organisationnelle » (Mikes et Kaplan, 2015, p. 52). Il est donc fondamental d'intégrer des mécanismes de contrôle automatisés, une gouvernance stricte des accès aux systèmes d'information et une organisation fonctionnelle claire (Vasarhelyi, Kogan et Tuttle, 2015 ; IFAC, 2022, p. 11).

Partant de ce constat, le présent article adopte une approche empirique pour analyser l'influence des mécanismes de contrôle de gestion sur le risque de fraude en contexte dématérialisé, en s'appuyant sur le cas de l'administration fiscale béninoise. Il interroge dans quelle mesure la reconfiguration des pratiques de contrôle, notamment en matière d'accès aux systèmes d'information, de conformité automatisée et de séparation fonctionnelle des tâches, permet de limiter les vulnérabilités associées à la digitalisation croissante des processus fiscaux.

La question centrale à laquelle cette recherche entend répondre est formulée comme suit : Quelle est l'influence des mécanismes de contrôle en contexte dématérialisé sur le risque de fraude dans l'administration fiscale au Bénin ?

Trois axes spécifiques en découlent :

- Évaluer l'effet du contrôle d'accès informatique sur le risque de fraude ;
- Examiner l'incidence du contrôle de conformité automatisé ;
- Mesurer l'influence de la séparation des tâches dans un environnement fiscal numérisé.

Cette étude vise à comprendre les interactions entre transformation numérique et dispositifs de contrôle pour renforcer la résilience fiscale face à la fraude et promouvoir une culture durable de conformité. Elle s'organise en quatre sections : revue critique de la littérature et hypothèses, méthodologie, résultats empiriques, puis analyse critique fondée sur les cadres théoriques.

1. Revue de littérature

Cette revue analyse l'impact de la transformation numérique sur les dispositifs de contrôle fiscal au Bénin, en lien avec la maîtrise des risques et la lutte contre la fraude. Elle comble le manque d'études sur l'articulation entre innovations technologiques et mécanismes classiques de contrôle en contexte dématérialisé, en explorant la résilience des systèmes fiscaux et les conditions d'une culture durable de conformité.

1.1. Fondements théoriques intégrés de l'analyse du risque de fraude en contexte fiscal dématérialisé

La digitalisation des administrations fiscales transforme profondément les modalités de contrôle, devenant un levier stratégique contre la fraude. Cette recherche mobilise un cadre théorique intégré combinant contrôle de gestion, sociologie des organisations, gouvernance publique et systèmes d'information, afin de mieux comprendre le risque en environnement numérique.

Le modèle s'appuie sur le référentiel COSO (2013), structuré autour de cinq composantes,

mais limité face aux motivations comportementales et aux asymétries d'information. La théorie de l'agence (Jensen et Meckling, 1976) souligne ces asymétries accrues, justifiant la traçabilité et l'imputabilité, tout en restant centrée sur les relations contractuelles. Krahel et Vasarhelyi (2014) considèrent la fraude comme multidimensionnelle, intégrant technologie, processus et comportements, appuyée par la chaîne de valeur du contrôle (Böhme et Moore, 2012), centrée sur les réponses organisationnelles.

Les modèles comportementaux de Cressey (1953) et de Wolfe et Hermanson (2004) expliquent les motivations individuelles, sans toutefois prendre en compte les dynamiques structurelles. L'approche sociotechnique (Emery et Trist, 1960 ; Le Moënne, 2015) articule technologies et systèmes sociaux, mais néglige parfois les logiques institutionnelles ou symboliques. L'approche néo-institutionnelle (DiMaggio et Powell, 1983) met en lumière les pressions mimétiques et coercitives qui poussent à adopter des innovations numériques par conformité plus que par efficacité.

La théorie du capital social (Putnam, 2000 ; Nahapiet et Ghoshal, 1998) alerte sur un effet paradoxal de la dématérialisation : la fragilisation des régulations informelles fondées sur la confiance et la vigilance partagée. Le modèle intègre trois dispositifs clés : le contrôle d'accès informatique (CAI) avec règles strictes (Sandhu et Samarati, 1994 ; Anderson, 2008), le contrôle de conformité automatisé (CCA) pour la détection continue d'anomalies (Böhme et Moore, op. cit.), et la séparation des tâches (ST) pour limiter abus et collusion (Reinhold, 2007 ; Whittington et Pany, 2016). Ces leviers, combinant contraintes techniques, dynamiques organisationnelles et comportements humains, soulignent la nécessité d'une approche holistique (Albrecht et al., 2012).

1.2. Mécanismes de contrôle numérique et défis organisationnels en contexte dématérialisé

Dans un environnement dématérialisé, la lutte contre la fraude s'appuie sur trois leviers technologiques : la digitalisation du contrôle d'accès, l'automatisation des contrôles et la séparation des fonctions.

Le contrôle d'accès numérique, via identifiants et habilitations strictes, limite les intrusions et assure la traçabilité (Dhillon et Moores, 2001 ; Whitman et Mattord, 2010). Les journaux de

connexion renforcent l'imputabilité (D'Arcy et al., 2009 ; ISACA, 2019) et doivent respecter les normes ISO/IEC 27001 (2013) avec audits réguliers (Cebula et Young, 2010 ; Payne, 2014). L'Estonie et le Chili illustrent l'efficacité de l'authentification forte (OCDE, 2022), malgré des failles comme le partage de mots de passe (Kankanhalli et al., 2003 ; OCDE, 2019). La blockchain offre également des garanties élevées d'intégrité (Crosman, 2017 ; Hertig, 2020).

L'automatisation permet la détection en temps réel d'anomalies et de fraudes complexes (OCDE, 2017 ; Caudill et al., 2021 ; Geradin et Kuschel, 2020 ; Wenzel et al., 2020), mais soulève des questions sur les biais des systèmes auto-apprenants (Pasquale, 2015). Le succès dépend de la qualité des données et de leur appropriation par les agents (Cordella et Tempini, 2015 ; Heeks, 2017 ; Arvidsson et al., 2022).

La séparation des fonctions (SoD), pilier du contrôle antifraude (COSO, ibid. ; Bouquin, 2023 ; Jensen, 2019), s'appuie sur des droits différenciés et des alertes croisées (Weill et Ross, 2005). Son efficacité est cependant affaiblie par des pratiques informelles (Granlund, 2011 ; Quattrone, 2016 ; ISACA, op. cit.), notamment en Afrique où les ressources sont limitées (Diabaté et al., 2020 ; Mbengue et al., 2022). Le numérique renforce ces mécanismes à condition qu'ils soient intégrés de manière cohérente dans une gouvernance efficace.

1.3. Revue empirique et formulation des hypothèses de recherche

Vasarhelyi, Kogan et Tuttle (2015) montrent que les dispositifs de contrôle d'accès — identifiants personnels, droits différenciés, authentification multifactorielle — limitent l'exposition aux risques de manipulation des données fiscales. En Afrique, Gupta (2021) observe que « l'absence de politique d'accès structurée est un vecteur clé de fraude dans les régies financières digitalisées » (p. 42). La restriction des droits d'accès selon les responsabilités permet de tracer les opérations et d'en identifier les auteurs.

Hypothèse H1 : Le contrôle d'accès informatique réduit le risque de fraude dans l'administration fiscale au Bénin.

1.3.2. Contrôle automatisé et conformité accrue

L'automatisation des contrôles, par le biais d'algorithmes de recoupement, d'alertes en cas d'anomalies ou de validations systématiques, favorise la détection précoce des erreurs et des fraudes. L'IFAC (2022), ainsi que Flowerday et Tuyikeze (2016), démontrent que ces dispositifs limitent les marges de manœuvre pour les manipulations humaines. L'expérience de la Rwanda Revenue Authority (2020) révèle que la généralisation du système e-Tax a permis d'accroître les recettes fiscales de 18 % en deux ans.
Hypothèse H2 : Le contrôle de conformité automatisé contribue positivement à la réduction du risque de fraude dans l'administration fiscale au Bénin.

1.3.3. Séparation des tâches et transparence organisationnelle

La séparation des fonctions, recommandée par le cadre COSO, permet de prévenir les collusions et les abus de pouvoir. En environnement numérique, elle se traduit par des workflows différenciés, des responsabilités partagées et une supervision automatisée. Mikes et Kaplan (2015) notent que, dans les administrations fiscales européennes, « la traçabilité des responsabilités est un dissuasif efficace contre les collusions internes » (p. 61).
Hypothèse H3 : La séparation des tâches en environnement fiscal numérique réduit les opportunités de fraude interne.

2. Méthodologie de la recherche de terrain

Afin d'examiner empiriquement l'influence des mécanismes de contrôle numérique sur le risque de fraude dans l'administration fiscale béninoise, cette recherche adopte une démarche mixte séquentielle (Creswell & Plano Clark, 2017), combinant une phase qualitative exploratoire suivie d'une phase quantitative confirmatoire. Cette approche permet de croiser la profondeur d'analyse des discours avec la robustesse statistique, renforçant ainsi la validité interne et externe des résultats.

2.1. Phase qualitative : entretiens exploratoires

La première phase repose sur 15 entretiens semi-structurés menés auprès d'agents fiscaux et de cadres de la Direction Générale des Impôts (DGI), incluant la Direction des Grandes Entreprises (DGE), la Cellule des Factures Normalisées et plusieurs Centres des impôts. Le

guide d'entretien a été construit à partir de la littérature et des cadres théoriques mobilisés (COSO, 2013 ; Cressey, 1953 ; Wolfe & Hermanson, 2004), et visait à explorer les représentations et pratiques liées à trois dispositifs : contrôle d'accès informatique (CAI), contrôle de conformité automatisé (CCA) et séparation des tâches (ST).

Les données verbatim recueillies ont été analysées selon une approche thématique (Braun & Clarke, 2021), enrichie par un traitement lexicométrique via Python. L'analyse abductive (Kuckartz, 2014) a permis de dégager quatre catégories centrales : rôle du contrôle humain, rigidité et potentialités du contrôle automatisé, institutionnalisation progressive des processus numériques, et arbitrages éthiques face aux contraintes organisationnelles. Ces résultats ont servi de base à la formulation opérationnelle des hypothèses de recherche et à la construction du questionnaire quantitatif.

2.2. Phase quantitative: enquête par questionnaire

Dans un second temps, une enquête par questionnaire structuré a été conduite auprès de 305 agents de la DGI, sur une population cible estimée à 350 individus directement impliqués dans la dématérialisation des procédures fiscales. L'échantillonnage stratifié proportionnel a pris en compte les principales unités organisationnelles (DGE, Cellule des Factures Normalisées, services centraux et déconcentrés). Le taux de réponses exploitables atteint 87,14 %, assurant la représentativité de l'échantillon et la robustesse des analyses multivariées (Hair et al., 2019).

Le questionnaire, élaboré à partir de la phase qualitative et validé par deux experts en fiscalité et contrôle interne, comportait 28 items mesurés sur une échelle de Likert à trois points (1 = désaccord, 2 = neutre, 3 = accord). Ce choix réduit les biais de désirabilité sociale fréquents dans des environnements hiérarchisés (Joshi et al., 2015) et facilite l'interprétation statistique en contexte professionnel. Les variables (voir tableau 1) ont été structurées comme suit :

- Variable dépendante : perception du risque de fraude (manipulation de données, falsification documentaire, cyberfraude).
- Variables indépendantes : contrôle d'accès informatique (authentification multifactorielle, gestion différenciée des droits), contrôle de conformité automatisé

(recoupements algorithmiques, alertes automatiques), séparation des tâches (workflows différenciés, responsabilités partagées).

- Variables de contrôle : âge, sexe, ancienneté et niveau d'instruction des agents.

Tableau 1 : Les variables de notre recherche

Catégorie	Variables	Indicateurs / Mesures	Références
Variable dépendante	Risque de fraude (RF)	Manipulation de données, falsification de documents fiscaux, cyberfraude perçue	Mungai & Otieno (2023) ; Zheng et al. (2022)
Variables indépendantes	Contrôle d'accès informatique (CAI)	Authentification multifactorielle, gestion différenciée des droits, traçabilité	Becerra & Gupta (2023) ; COSO (2013)
	Contrôle de conformité automatisé (CCA)	Recoupements algorithmiques, alertes automatiques, validations systématiques	Flowerday & Tuyikeze (2016) ; IFAC (2022)
	Séparation des tâches (ST)	Workflows différenciés, responsabilités partagées, supervision automatisée	Arens et al. (2014) ; Whittington & Pany (2016)
Variables de contrôle	Caractéristiques sociodémographiques	Âge, sexe, ancienneté dans la fonction, niveau d'instruction	-

Source : Les auteurs

Ainsi, la combinaison d'un échantillonnage rigoureux, d'un questionnaire validé et d'une structuration claire des variables fournit un cadre méthodologique robuste, garantissant la qualité des données collectées et leur pertinence pour analyser l'influence des mécanismes de

contrôle numérique sur le risque de fraude.

2.3. Méthodes d'analyse des données

Le traitement des données a été effectué à l'aide du logiciel SPSS 26, qui offre des fonctionnalités adaptées aux analyses multivariées en sciences de gestion. L'approche a combiné plusieurs outils statistiques complémentaires afin de garantir la fiabilité et la validité des résultats.

Dans un premier temps, une analyse factorielle exploratoire (AFE) a été conduite pour vérifier la validité des construits et identifier les dimensions latentes sous-jacentes aux 28 items du questionnaire. Le test de Bartlett de sphéricité et l'indice KMO (Kaiser-Meyer-Olkin) ont confirmé la pertinence de l'AFE, en indiquant un niveau d'adéquation satisfaisant pour le traitement factoriel. Les saturations factorielles supérieures à 0,5 ont validé la convergence des items au sein de leurs dimensions respectives, tandis que la différenciation entre facteurs a assuré la validité discriminante.

Dans un deuxième temps, la fiabilité interne des échelles a été évaluée à l'aide du coefficient alpha de Cronbach. Les valeurs obtenues, comprises entre 0,63 et 0,78, traduisent une fiabilité allant d'acceptable à bonne, en cohérence avec les standards psychométriques établis (Nunnally & Bernstein, 1994). Ces résultats confortent la robustesse de l'outil de mesure.

Ensuite, des analyses de corrélation de Pearson ont été réalisées afin d'examiner la force et la direction des relations linéaires entre la variable dépendante (risque de fraude) et les trois mécanismes de contrôle étudiés. Cette étape a permis d'identifier les associations les plus pertinentes à approfondir par la modélisation.

Enfin, une régression linéaire multiple a été mise en œuvre pour estimer l'effet propre de chaque mécanisme de contrôle sur le risque de fraude, selon le modèle :

$$RF = \beta_0 + \beta_1 CAI + \beta_2 CCA + \beta_3 ST + \varepsilon$$

Ce modèle a permis de hiérarchiser l'influence relative des trois dispositifs et d'en évaluer la significativité statistique. Le recours à la régression multiple est justifié par sa capacité à isoler l'impact de chaque variable indépendante tout en contrôlant les effets des autres.

Ainsi, l'utilisation combinée de l'AFE, des tests psychométriques, des corrélations et de la

régression garantit la rigueur de l'analyse et assure que les relations identifiées entre les mécanismes de contrôle et le risque de fraude reposent sur des bases statistiques solides et interprétables.

3. Rsultats

3.1. Résultats de l'étude qualitative

L'analyse qualitative repose sur une démarche inductive, fondée sur l'analyse thématique telle que définie par Braun et Clarke (2021). Cette approche permet de structurer les données issues des entretiens semi-structurés autour de catégories signifiantes, en cohérence avec le cadre conceptuel mobilisé. Elle vise à faire émerger le sens attribué par les agents fiscaux aux dispositifs de contrôle numérique dans un contexte de dématérialisation. Afin de renforcer la validité de l'interprétation, l'analyse thématique a été complétée par une analyse lexicométrique appuyée sur un traitement informatique des corpus (via Python), dont les nuages de mots ont permis de visualiser les récurrences lexicales et les cooccurrences significatives. Cette triangulation méthodologique – combinant codage thématique et exploration lexicale – accroît la robustesse des résultats et assure une meilleure saturation des données qualitatives.

3.1.1. Analyse thématique des données

L'exploitation des verbatim révèle quatre axes majeurs, traduisant les représentations, tensions et pratiques des acteurs fiscaux vis-à-vis des dispositifs de contrôle numérique. Ces axes ne doivent pas être compris comme des catégories exclusives, mais plutôt comme des pôles interprétatifs structurant la perception des enquêtés.

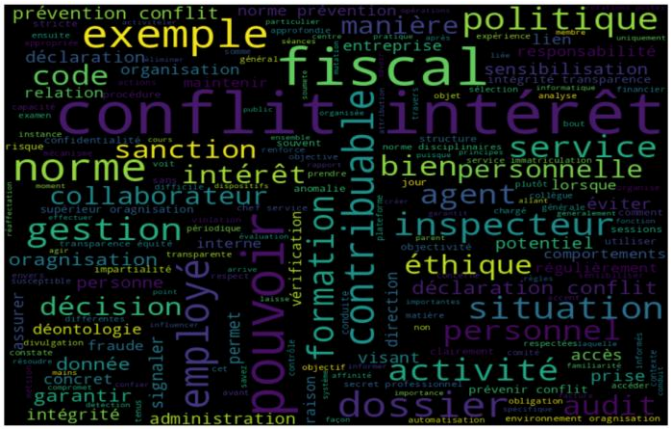
Contrôle direct : la prééminence du facteur humain

L'analyse des discours révèle une valorisation marquée du contrôle direct, considéré par les agents fiscaux comme une garantie incontournable dans un environnement fortement numérisé. Les termes les plus fréquemment mobilisés – « supervision », « vigilance », « formation » et « efficacité » – traduisent une conviction largement partagée : l'intervention humaine demeure indispensable pour assurer la fiabilité et la sécurisation des processus. Cette

insistance souligne le rôle irremplaçable de l'expertise et du discernement des acteurs dans la prévention de la fraude, en complément des dispositifs numériques.

Toutefois, cette centralité du facteur humain s'accompagne d'une fragilité structurelle. L'intervention est souvent conçue dans une logique ponctuelle et réactive, plutôt qu'inscrite dans une stratégie systémique d'anticipation des risques. En conséquence, son efficacité se limite à des corrections a posteriori, sans parvenir à instaurer une dynamique préventive durable. La figure 1 illustre cette perception en représentant les mesures associées à la prévention des conflits d'intérêts, où l'importance de la vigilance humaine ressort nettement, mais demeure faiblement intégrée à des mécanismes organisationnels de long terme.

Figure 1: Représentation associée aux mesures de prevention des conflicts d'intérêts



Source : *Auteurs à partir des verbatim, traitement Python*

Contrôle indirect : institutionnalisation des processus numériques

Les acteurs expriment une perception ambivalente à l'égard du contrôle indirect, incarné par les algorithmes de détection d'anomalies et les interfaces numériques prescriptives. D'un côté, il est perçu comme un facteur de rigueur et de rationalisation, en réduisant l'arbitraire et en instaurant une forme d'impartialité technique. De l'autre, sa rigidité face aux cas atypiques ou aux situations non standardisées limite son efficacité. Cette tension met en lumière le besoin d'articuler l'objectivité technique des systèmes numériques avec l'expertise interprétative des agents, afin d'éviter que les anomalies détectées ne restent sans mise en contexte ni résolution

appropriée.

Contrôle automatisé : efficacité mais rigidité

Les entretiens reconnaissent au contrôle automatisé une efficacité indéniable dans la détection précoce des comportements frauduleux. Les algorithmes de gestion des risques et les formulaires numériques contraints permettent en effet de verrouiller certaines pratiques frauduleuses et de générer des alertes rapides. Cependant, les limites de l'automatisation apparaissent clairement : incapacité à prendre en compte des scénarios complexes, dépendance à la qualité des données saisies, difficulté à traiter des situations inédites. Les agents insistent ainsi sur la nécessité de considérer ces dispositifs non pas comme des substituts, mais comme des compléments à l'expertise humaine, seule capable d'introduire nuance, contextualisation et jugement critique.

Apports de l'analyse lexicométrique

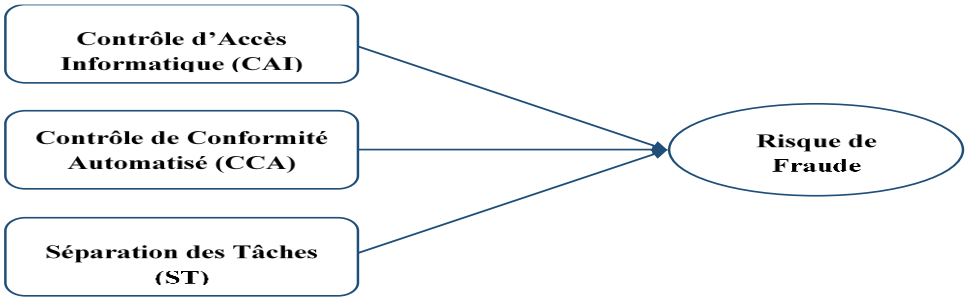
L'analyse lexicométrique vient approfondir les résultats issus du codage thématique en révélant la récurrence de termes tels que « maîtrise humaine », « gestion du risque de fraude », « technologie » ou encore « dilemmes éthiques ». Ces régularités lexicales mettent en évidence un déséquilibre latent dans les représentations des agents fiscaux : si la digitalisation est largement perçue comme un vecteur de modernisation et d'efficacité, elle tend simultanément à reléguer la dimension humaine et délibérative au second plan, alors même que les praticiens insistent sur son caractère indispensable. Ce constat souligne la tension centrale entre rationalité technologique et jugement humain, et interroge sur les conditions organisationnelles nécessaires pour parvenir à un équilibre durable dans la gouvernance des systèmes fiscaux numérisés.

Ces enseignements qualitatifs constituent le socle du modèle théorique élaboré dans cette recherche. Celui-ci conçoit le risque de fraude comme une variable systémique (Beasley et al., 2009 ; Krahel & Vasarhelyi, 2014), en s'appuyant sur le référentiel COSO (2013). Il repose sur le triptyque prévention–détection–réaction (Böhme & Moore, 2012) et intègre les bénéfices de l'automatisation dans la réduction des vulnérabilités numériques (Vasarhelyi & Halper, 1991). Trois leviers sont ainsi mis en avant : le contrôle d'accès informatique (Sandhu

& Samarati, 1994 ; Anderson, 2008), le contrôle continu automatisé (Böhme & Moore, 2012) et la séparation des tâches (Reinhold, 2007 ; Whittington & Pany, 2016). L'ensemble, tout en prolongeant le triangle de la fraude (Cressey, 1953), invite à une relecture intégrée qui combine contraintes techniques, logiques organisationnelles et comportements humains (Albrecht et al., 2012).

Cette articulation est synthétisée dans le modèle conceptuel présenté à la figure 2, lequel illustre la dynamique entre dispositifs de contrôle et maîtrise du risque de fraude en contexte dématérialisé.

Figure 2: Modèle conceptuel d'articulation entre dispositifs de contrôle et risque de fraude



Source : Conception des auteurs à partir de la littérature et des résultats empiriques (2023)

3.2. Résultats de l'étude quantitative

3.2.1. Répartition géographique et profil des répondants

L'analyse des caractéristiques sociodémographiques des répondants met en évidence une forte concentration dans les départements du Littoral (40,7 %) et de l'Atlantique (34,4 %), alors que le Plateau (3,9 %) et le Zou (5,9 %) sont faiblement représentés, ce qui traduit une couverture géographique inégale. L'échantillon est majoritairement masculin (68 %) et composé d'agents jeunes et en milieu de carrière, dont 52,8 % sont âgés de 35 à 44 ans. Le niveau d'instruction est globalement élevé, puisque 72,5 % des enquêtés détiennent un Master, dont 83,6 % sont spécialisés en fiscalité. Plus de la moitié des répondants justifient d'une expérience professionnelle supérieure à six ans. Toutefois, la faible représentation des cadres supérieurs et des titulaires d'un doctorat (1,3 %) limite la diversité des points de vue stratégiques dans l'échantillon.

Tableau 1 : Caractéristiques sociodémographiques et professionnelles des répondants

Variable	Modalité	Effectif (n)	Pourcentage (%)
Département d'affectation	Littoral	31	40,70 %
	Atlantique	26	34,42 %
	Zou	4	5,90 %
	Plateau	3	3,93 %
	Autres	12	15,05 %
Sexe	Masculin	52	68,00 %
	Féminin	24	32,00 %
Tranche d'âge	Moins de 35 ans	15	19,73 %
	35-44 ans	40	52,79 %
	45 ans et plus	20	27,48 %
Niveau instruction	Licence	10	13,12 %
	Master	55	72,46 %
	Doctorat	1	1,31 %
	Autres	10	13,12 %
Fonction	Fiscalistes	63	83,61 %
	Informaticiens	6	7,95 %
	Autres (auditeurs, juristes, etc.)	6	7,44 %
Expérience professionnelle	Moins de 6 ans	30	39,34 %
	6 ans et plus	46	60,66 %
Total		305	100,00

Source : Données de l'enquête quantitative (2023)

3.2.2. Méthodes d'analyse des données

Analyse factorielle

L'Analyse Factorielle Exploratoire (AFE) a permis d'identifier les structures latentes associées aux mécanismes de contrôle étudiés. Les tests préliminaires (KMO supérieur à 0,6

et test de Bartlett significatif) confirment la pertinence de l'AFE. Les résultats montrent une cohérence interne allant de modérée à bonne, avec des alphas de Cronbach compris entre 0,63 et 0,78. La séparation des tâches et le risque de fraude présentent des variances expliquées particulièrement élevées (76,27 % et 67,2 % respectivement).

Tableau 2 : Résultats d'analyse factorielle des variables liées à la gestion du risque

Echelle de mesure	Alpha de Cronbach	Analyse des items	Facteurs principaux	Variance expliquée
Contrôle d'Accès Informatique (CAI)	0,669	- L'item CAI2 diminue légèrement l'alpha - Bonne cohérence des autres items	5 facteurs extraits	-
Contrôle de Conformité Automatisé (CCA)	0,651	- Suppression de CCA6 sans effet notable - Faible contribution de CCA4 et CCA5	6 facteurs extraits	-
Séparation des Tâches (ST)	0,782	- Contributions fortes de ST5, ST1, ST4 - Variance marginale pour les autres items	3 facteurs extraits	76,27 %
Risque de Fraude (RF)	0,634	- Faible contribution de RF4 - Contribution forte de RF5	3 facteurs extraits	67,20 %
Vérification conditions	-	- KMO > 0,6 - Bartlett significatif	-	-

Source : Extrants statistiques sous SPSS 26 (2023)

Analyse de corrélation

Les corrélations de Pearson permettent d'examiner les relations linéaires entre les variables. Les résultats indiquent que le risque de fraude (RF) est faiblement mais significativement corrélé avec le contrôle d'accès informatique (CAI) ($r = 0,159$; $p = 0,005$), alors qu'aucune corrélation significative n'apparaît avec le contrôle de conformité automatisé (CCA) ni avec la séparation des tâches (ST).

Tableau 3 : Corrélations linéaires entre les variables

	RF	CAI	CCA	ST
RF	1	0,159**	-0,035	0,041
CAI		1	0,249**	0,493**
CCA			1	0,081
ST				1

Source : Extrants statistiques sous SPSS 26 (2023)

(p < 0,01)

Analyse de régression

Le modèle de régression linéaire multiple a été estimé afin de hiérarchiser l'impact des trois mécanismes de contrôle sur le risque de fraude. Les résultats montrent que seul le contrôle d'accès informatique (CAI) exerce un effet significatif et positif, tandis que le CCA et la ST n'ont pas d'influence statistiquement avérée.

Tableau 4 : Estimation du modèle linéaire entre RF et les variables indépendantes

Variables	Coefficients	Std. Error	t de Student	Significativité
(Constant)	1,037E-16	0,057	0,000	1,000
CAI	0,206	0,067	3,066	0,002
CCA	-0,082	0,059	-1,406	0,161
ST	-0,053	0,065	-0,819	0,413

Source : Extrants statistiques sous SPSS 26 (2023)

Validation des hypothèses

Les résultats empiriques confirment partiellement les hypothèses de départ. Le CAI joue un rôle significatif, mais le CCA et la ST ne montrent pas d'effets mesurables dans le contexte étudié.

Tableau 5 : Résultats de validation des hypothèses

N°	Hypothèse	Résultats empiriques clés	Dcision
H1	Le contrôle d'accès informatique réduit le risque de fraude	Corrélation significative (r = 0,159 ; p < 0,005) Régression positive et significative (β = 0,206 ; p = 0,002)	Confirmée
H2	Le contrôle de conformité automatisé réduit le risque de fraude	Corrélation faible (r = -0,035 ; p = 0,538) Régression non significative (β = -0,082 ; p = 0,161)	Rejetée
H3	La séparation des tâches réduit le risque de fraude	Corrélation faible (r = 0,041 ; p = 0,470) Régression non significative (β = -0,053 ; p = 0,413)	Rejetée

Source : Auteurs, sur la base des extrants statistiques (SPSS 26, 2023)

4. Discussion des résultats

Les résultats mettent en lumière la complexité de l'efficacité des mécanismes de contrôle en contexte dématérialisé. Loin de fournir une réponse univoque, ils invitent à une lecture nuancée, croisant les dimensions sociotechniques, institutionnelles et cognitives. Cette pluralité souligne la nécessité d'une approche intégrative qui dépasse une vision strictement instrumentale du contrôle et valorise la complémentarité entre technologie, organisation et comportements humains.

4.1. Analyse critique de l'influence des mécanismes de contrôle sur le risque de fraude

Contrôle d'accès informatique. La dématérialisation fiscale au Bénin complexifie les fraudes et remet partiellement en cause la pertinence du triangle de la fraude (Cressey, 1953). Le modèle du diamant, qui intègre la capacité à frauder, apparaît plus adapté (Wolfe & Hermanson, 2004). Les entretiens montrent que certains agents, maîtrisant SQL, logs et workflows, exploitent l'asymétrie d'information pour contourner les contrôles et asseoir un pouvoir discret. Comme l'a affirmé un inspecteur de CIME 1 Littoral : *« Les mécanismes de contrôle assurent une détection précoce des signaux de fraude. En contrôlant régulièrement les activités de l'entreprise, ils permettent d'identifier rapidement des anomalies ou des schémas inhabituels. »* Toutefois, ces dispositifs techniques restent insuffisants sans gouvernance cohérente et supervision active. Ce constat rejoint la théorie de l'agence (Jensen

& Meckling, 1976) et les approches sociotechniques (Power, 2013), qui rappellent que l'efficacité du contrôle repose autant sur la culture organisationnelle que sur les outils numériques.

Contrôle de conformité automatisé. Les résultats indiquent que l'automatisation, bien qu'elle repose sur des règles et alertes automatiques, souffre de rigidités algorithmiques, de données de qualité variable et d'une complexité fiscale difficilement modélisable. COSO (2013) insiste sur la nécessité d'une articulation claire entre contrôle et supervision, condition rarement remplie. Henri (2021) souligne de son côté les effets négatifs d'une faible maîtrise locale et de choix politiques inadéquats. Vaessen et al. (2022) rappellent que l'automatisation sous-estime la capacité des agents à contourner les règles, tandis qu'Orlikowski (2020) alerte sur les dérives d'une approche sociotechnique mal adaptée. Enfin, Putnam (2020) met en avant l'importance de la confiance sociale, fragilisée par une numérisation mal appropriée. Les témoignages confirment ces limites : *« Il faut s'assurer que les taux sont appliqués correctement et vérifier la saisie des données pour éviter les fraudes »* (inspecteur, CIME 1 Littoral). Un autre précise : *« Les systèmes automatisés attribuent des scores de risque aux contribuables, permettant une allocation plus efficace des ressources d'audit »* (inspecteur, CIME 2 Littoral). L'efficacité dépend donc d'une gouvernance locale renforcée et d'un investissement en formation continue.

Séparation des tâches. Principe fondateur du contrôle interne, la séparation des fonctions reste partiellement appliquée, notamment dans les unités à effectifs réduits où le cumul des responsabilités fragilise les dispositifs. La dématérialisation offre des atouts indéniables (traçabilité, accès différenciés), mais des pratiques comme le partage de mots de passe en réduisent la portée. Le cadre théorique mobilisé (COSO, théorie de l'agence, modèles de la fraude, approche sociotechnique) montre que l'appropriation des outils numériques demeure faible et que les logiques informelles persistent. Comme le soulignent Power (2007) et Moisdon (2022), l'efficacité du contrôle ne repose pas uniquement sur la technologie mais sur une redéfinition des rôles, un renforcement des compétences et une gouvernance axée sur l'intégrité.

4.2. Analyse des résultats à la lumière des modèles théoriques

L'évaluation des résultats mobilise plusieurs modèles théoriques de gestion du risque de fraude, adaptés au contexte africain. Le modèle de contrôle organisationnel insiste sur la maîtrise des technologies numériques et du contrôle des accès. Un chef de service déclare : *« Le contrôle d'accès informatique devient impératif »*, confirmant les conclusions de Bierstaker et al. (2006). Toutefois, la séparation des tâches s'avère peu efficace en l'absence d'outils numériques adéquats.

Le modèle de dissuasion (Becker, 1968) se heurte aux limites d'une faible spécialisation fonctionnelle et d'un déficit de compétences techniques. Le modèle de conformité volontaire (Allingham & Sandmo, 1972) reste affaibli par la faible confiance institutionnelle et le manque de coordination interne. Sur le plan sociologique, la surveillance sociale et culturelle (Durkheim, 1893 ; Schein, 1985) rappelle que les dispositifs techniques doivent être appropriés par l'organisation et intégrés dans des normes collectives.

Le référentiel COSO (2013) révèle un écart entre le potentiel technique et sa mise en pratique, souvent entravée par l'opacité des systèmes et l'absence de ségrégation stricte des fonctions. Dufresne & Mermoud (2017) soulignent que l'introduction de solutions comme le *data mining* ou l'intelligence artificielle explicable renforcerait la détection des anomalies. De même, le référentiel COBIT (ISACA, 2019) prescrit une gouvernance numérique rigoureuse, mais son application reste limitée par des vulnérabilités organisationnelles.

Enfin, selon le modèle d'innovation de Rogers (2003), l'adoption des technologies est freinée par les résistances internes et le déficit de formation. Un responsable fiscal souligne : *« Le contrôle automatisé des déclarations permet d'éviter que des données erronées parviennent à l'administration »*, mais cette efficacité reste conditionnée par une mise en œuvre rigoureuse et une appropriation effective.

Si ces modèles offrent des cadres analytiques pertinents, leur application au contexte numérique africain appelle une démarche intégrée combinant innovation technologique, transformation organisationnelle et adaptation culturelle. Seule une telle approche peut renforcer durablement l'efficacité des dispositifs de contrôle fiscal et la lutte contre la fraude.

4.3. Profil des répondants et contrôle fiscal dématérialisé

1. La forte concentration des répondants dans les départements du Littoral et de l'Atlantique, qui constituent les principaux pôles fiscaux du pays, confère une pertinence empirique particulière à l'étude. Le profil des participants, majoritairement composé de fiscalistes titulaires d'un Master, permet une analyse approfondie des mécanismes de contrôle tels que le Contrôle d'Accès Informatique (CAI), le Contrôle de Conformité Automatisé (CCA) et la Séparation des Tâches (ST). Ces dispositifs s'inscrivent directement dans les cadres de référence proposés par le COSO (2013) et la théorie de l'agence (Jensen & Meckling, 1976), en soulignant l'importance de la traçabilité et de l'imputabilité dans la lutte contre la fraude.

2. Toutefois, la faible représentation des cadres supérieurs et des docteurs limite l'exploration des dimensions stratégiques du contrôle. Or, celles-ci sont centrales dans les approches néo-institutionnelle (DiMaggio & Powell, 1983), sociotechnique (Emery & Trist, 1960 ; Le Moënne, 2015) et du capital social (Putnam, 2000 ; Nahapiet & Ghoshal, 1998), qui insistent sur l'appropriation institutionnelle, la culture organisationnelle et la confiance partagée. Cette limite restreint la capacité d'analyse de l'intégration des innovations numériques dans les logiques organisationnelles et institutionnelles qui façonnent la lutte contre la fraude fiscale.

4.4. Modèle de recherche empirique intégré

La discussion des résultats conduit à la proposition d'un modèle empirique intégré visant à renforcer le contrôle de la fraude en contexte fiscal dématérialisé, tout en tenant compte des spécificités africaines. Ce modèle hybride et évolutif repose sur plusieurs axes stratégiques.

Premièrement, il préconise la mise en place d'un comité de gouvernance numérique rassemblant fiscalistes, informaticiens, auditeurs et experts en cybersécurité. Ce comité aurait pour mission d'aligner la digitalisation des processus fiscaux sur la lutte contre la fraude, d'intégrer la gestion des risques dans les projets informatiques et de renforcer les audits numériques grâce à l'usage du *data analytics* et de l'intelligence artificielle explicable.

Deuxièmement, le contrôle d'accès informatique doit être renforcé par la création de profils personnalisés intégrant une authentification forte (biométrie, OTP) et par la mise en place de journaux de connexion systématiquement audités. Les agents devront être formés à la gestion de leur propre traçabilité afin de favoriser une logique d'auto-responsabilisation.

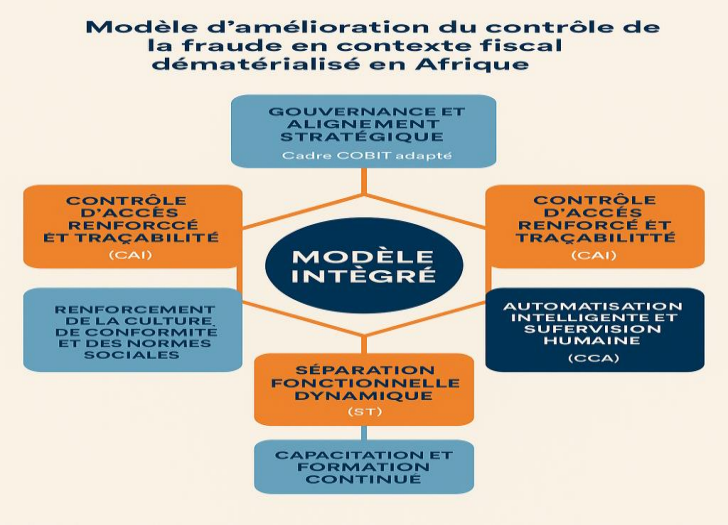
Troisièmement, les contrôles automatisés seront complétés par des vérifications humaines ciblées, appuyées sur un tableau de bord de supervision en temps réel accessible aux chefs de service. La séparation des tâches sera optimisée grâce à des workflows numériques et à l'utilisation d'ERP fiscaux, complétés par des tests d'intrusion organisationnels permettant de détecter d'éventuelles failles structurelles.

Quatrièmement, le modèle intègre une dimension culturelle et comportementale. Des campagnes de sensibilisation à l'intégrité numérique et des mécanismes de reconnaissance pour les comportements conformes seront développés, en lien avec les syndicats et associations de contribuables.

Enfin, la capacitation des agents constituera un pilier central. Elle passera par des formations certifiantes en audit numérique, cybersécurité et éthique digitale, enrichies par des simulations de fraude et un système de mentorat croisé.

Ce modèle dépasse ainsi une simple transposition des cadres occidentaux en tenant compte des contraintes africaines, telles que les budgets limités, la faible confiance institutionnelle et la nécessité d'un fort ancrage organisationnel.

Figure 3 : Modèle empirique intégré



Source : Auteurs, à partir de la littérature et des résultats de l'étude qualitative (2023)

Conclusion

Cette recherche a examiné l'influence des mécanismes de contrôle en contexte dématérialisé sur la réduction du risque de fraude au sein de l'administration fiscale béninoise. En mobilisant à la fois des entretiens semi-structurés et des analyses statistiques, elle a permis de croiser les perceptions des agents avec des validations empiriques, offrant une compréhension à la fois nuancée et robuste du phénomène. Les résultats montrent que la numérisation des processus fiscaux, bien qu'indispensable à la modernisation des administrations, ne constitue pas en elle-même une garantie contre la fraude. Mal encadrée, elle peut même générer de nouvelles vulnérabilités. L'efficacité des dispositifs numériques dépend donc étroitement des compétences des agents, de leur formation, de leur éthique professionnelle et de la qualité de la supervision exercée. La lutte contre la fraude fiscale ne peut ainsi être dissociée des dynamiques organisationnelles et culturelles propres aux contextes africains.

Sur le plan théorique, cette recherche dépasse les cadres normatifs classiques tels que le COSO (2013), centrés sur la conformité, en s'inscrivant dans une perspective critique inspirée des travaux de Power (1997) et Simons (1995). Elle plaide pour une approche systémique et contextualisée, articulant gouvernance, usage des technologies et logiques de pouvoir. Le référentiel COBIT (ISACA, 2019), bien qu'offrant des pistes intéressantes, doit être adapté aux réalités africaines, en tenant compte des contraintes structurelles et des valeurs organisationnelles locales.

D'un point de vue managérial, l'étude propose un modèle intégré d'amélioration du contrôle de la fraude en contexte fiscal dématérialisé. Ce modèle repose sur six axes : (1) une gouvernance numérique stratégique, (2) un contrôle d'accès et une traçabilité renforcés, (3) une automatisation intelligente mais supervisée, (4) une séparation fonctionnelle dynamique, (5) une culture de conformité et d'éthique partagée, et (6) une capacitation continue des acteurs. Il combine ainsi leviers technologiques et facteurs humains dans une logique d'alignement stratégique, d'agilité organisationnelle et de résilience face aux menaces émergentes.

Sur le plan épistémologique, l'usage d'une méthodologie mixte a confirmé la pertinence de combiner approches qualitatives et quantitatives pour appréhender des réalités complexes. Cette démarche a permis de valider les hypothèses tout en explorant des dimensions latentes souvent négligées par les études classiques. Certes, certaines limites demeurent, en particulier

quant à la généralisation des résultats et à la profondeur théorique de certains concepts émergents. Néanmoins, cette recherche constitue une base solide pour l'élaboration de politiques publiques plus efficaces, capables d'intégrer les spécificités des contextes africains et d'accompagner les transformations numériques et sociétales en cours.

Bibliographie

Albee, A., Hesse, C. et Tetteh, E., 2021. Digitalisation and Revenue Mobilisation in Africa, African Tax Administration Forum, Pretoria.

Albrecht, W.S., Albrecht, C.C., Albrecht, C.O. et Zimbelman, M.F., 2012. Fraud Examination, South-Western Cengage Learning, Boston, 4e éd., 720 p.

Allingham, M. G. et Sandmo, A., 1972. Income tax evasion : A theoretical analysis, North-Holland Publishing Company, Amsterdam.

Anderson, R., 2008. Security Engineering : A Guide to Building Dependable Distributed Systems, Wiley, New York, 2e éd., 1080 p.

Arens, A.A., Elder, R.J. et Beasley, M.S., 2014. Auditing and Assurance Services : An Integrated Approach, Boston : Pearson, 15e édition.

Banque mondiale, 2022. Les réformes numériques pour une mobilisation efficace des recettes fiscales, Washington, D.C., p. 19.

Beasley, M. S., Carcello, J. V., Hermanson, D. R., et Neal, T. L. (2009). « The audit committee oversight process », Contemporary Accounting Research, Toronto, Vol. 26, pp. 65–122.

Becerra, M. et Gupta, A., 2023. « Multifactor Authentication and Fraud Reduction in Tax Administration », Journal of Information Security and Applications, Londres, vol. 70, janvier, pp. 102–115.

Becker, G. S., 1968. Crime and Punishment : An Economic Approach, University of Chicago Press, Chicago.

Bierstaker, J., Brody, R. G. et Pacini, C., 2006. « Accountants' perceptions regarding fraud detection and prevention methods », Managerial Auditing Journal, Bingley, Vol. 21, n°5, pp. 520–535.

Böhme, R. et Moore, T., 2012. « The economics of information security », Science, Washington D.C., vol. 339, février, pp. 610–613.

Böhme, R., et Moore, T. (2012). « The economics of cyber security : Principles and policy options », International Journal of Critical Infrastructure Protection, Elsevier, Vol. 4, pp. 103–117.

Bouquin, H., 2023. Le contrôle de gestion, PUF, Paris, 11e éd., 672 p.

Braun, V., et Clarke, V. (2021). Thematic Analysis : A Practical Guide. London : SAGE Publications.

Bryman, A., 2016. Social Research Methods, Oxford : Oxford University Press, 5e édition.

Caudill, R., Liang, Y., Watson, D. et Wu, Y., 2021. « Real-time anomaly detection in digital taxation systems », Journal of Information Systems, New York, vol. 35, n°1, pp. 45–67.

Cebula, J.J. et Young, L.R., 2010. A taxonomy of operational cyber security risks, Carnegie Mellon University, Pittsburgh, CERT, 52 p.

Cordella, A. et Tempini, N., 2015. « E-government and organizational change: Reappraising the role of ICT and bureaucracy in public service delivery », Government Information Quarterly, Amsterdam, vol. 32, n°3, pp. 279–286.

COSO. (2013). Internal Control — Integrated Framework. Durham : Committee of Sponsoring Organizations of the Treadway Commission.

Cour des comptes, 2019. Rapport public annuel, Cotonou.

Cour des comptes, 2021. Rapport public annuel, Cotonou.

Cressey, D. R. (1953). Other People's Money : A Study in the Social Psychology of Embezzlement. Glencoe : Free Press.

Creswell, J.W. et Plano Clark, V.L., 2017. Designing and Conducting Mixed Methods Research, Los Angeles : SAGE Publications, 3e édition.

Crosman, P., 2017. « Blockchain : Reimagining clearing and settlement », American Banker, New York, janvier, pp. 22–26.

D'Arcy, J., Hovav, A. et Galletta, D., 2009. « User awareness of security countermeasures and its impact on information systems misuse : A deterrence approach », Information Systems Research, Baltimore, vol. 20, n°1, pp. 79–98.

DGI, 2022. Rapport d'évaluation de la mise en œuvre de la facture normalisée, Cotonou, p. 3.

Dhillon, G. et Moores, S., 2001. « Computer crimes : Theorizing about the enemy within », Computers et Security, Oxford, vol. 20, n°8, pp. 715–723.

Diabaté, D., Sanogo, B. et Ouattara, L., 2020. « Digitalisation et performance des services fiscaux en Afrique de l'Ouest », Revue Africaine de la Comptabilité et de l'Audit, Abidjan, n° 12, juillet, pp. 45–66.

DiMaggio, P. J. et Powell, W. W., 1983. The Iron Cage Revisited : Institutional Isomorphism and Collective Rationality in Organizational Fields, American Sociological Review, Washington, Vol. 48, pp. 147–160.

Dolnicar, S., Grün, B. et Leisch, F., 2011. « Quick, simple and reliable : Three-point Likert scales », International Journal of Market Research, Londres, vol. 53, n° 2, mars, pp. 255–264.

Dufresne, M. et Mermoud, A., 2017. Audit interne et gestion des risques : Méthodes et outils pour une gouvernance efficace, Éditions d'Organisation, Paris.

Durkheim, E., 1893. De la division du travail social, Félix Alcan, Paris.

Emery, F. E. et Trist, E. L. (1960). Sociotechnical Systems. Londres : Tavistock Institute, 48 p.

Flowerday, S. et Tuyikeze, T. (2016). « Information privacy and security in the digital age : A South African context », Information et Computer Security, 24(4), 437–456.

Flowerday, S. et Tuyikeze, T. (2016). « Information security policy compliance : A user acceptance perspective », Computers et Security, 61, 1–14.

Flowerday, S. et Tuyikeze, T. (2016). « Information systems security and the need for policy enforcement through monitoring », South African Journal of Information Management, 18(1), 1–8.

FMI, 2021. Rwanda : Selected Issues, Washington, D.C., p. 25.

Geradin, D. et Kuschel, L., 2020. « Algorithmic enforcement and EU competition law », European Competition Journal, Londres, vol. 16, n°2-3, pp. 541–574.

Granlund, M., 2011. « Extending AIS research to management accounting and control issues : A research note », International Journal of Accounting Information Systems, Amsterdam, vol. 12, n°1, pp. 3–19.

Guba, E.G. et Lincoln, Y.S., 1989. Fourth Generation Evaluation, Newbury Park : SAGE Publications.

Gupta, A., 2021. « Digital transformation and fraud risks in African public finance », Journal of African Public Administration, Nairobi, vol. 6, n°1, avril, pp. 35–48.

Gupta, A., 2021. Fraud Risk Management in the Digital Age, New Delhi, Sage Publications.

Gupta, M., 2021. « Digital transformation and the emergence of new cyber risks in the public sector », Government Information Quarterly, Amsterdam, vol. 38, n° 3, p. 101–108.

Henri, J.-F., 2021. « Gouvernance numérique et contrôle de gestion : vers une approche intégrée », Revue Française de Comptabilité, Paris, n°559, avril, pp. 33-37.

IFAC, 2022. Harnessing digitalisation for better public financial management, New York, p. 11.

IGF, 2020. Rapport annuel de l'Inspection générale des finances, Cotonou.

International Federation of Accountants (IFAC), 2022. Automation and the Public Sector Accountant : Opportunities and Risks, New York, IFAC.

ISACA. (2019). COBIT 2019 Framework : Governance and Management Objectives. Schaumburg, IL : ISACA, 120 p.

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

Joshi, A., Kale, S., Chandel, S. et Pal, D.K., 2015. « Likert Scale : Explored and Explained », British Journal of Applied Science et Technology, Londres, vol. 7, n° 4, avril, pp. 396–403.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y. et Wei, K.K., 2003. « An integrative study of information systems security effectiveness », International Journal of Information Management, Amsterdam, vol. 23, n°2, avril, pp. 139–154.

Kaplan, R. S. et Mikes, A., 2015. « Risk Management — The Revealing Hand », Journal of Applied Corporate Finance, New York, vol. 27, n°1, hiver, pp. 8-18.

Kirchler, E., 2007. « The economic psychology of tax behaviour », Cambridge University Press, Cambridge, vol. 1, p. 1–243.

Krahel, J. P., et Vasarhelyi, M. A. (2014). « AIS as a facilitator of accounting change : Technology, practice, and education », Journal of Information Systems, Sarasota, Vol.

28, n°2, pp. 1–15.

Kuckartz, U., 2014. Qualitative Text Analysis : A Guide to Methods, Practice et Using Software, Londres : SAGE Publications.

Le Moënne, C., 2015. Les dispositifs sociotechniques, Presses des Mines, Paris, 270 p.

Le Moënne, C., 2015. Les organisations entre logiques d'action et logiques d'interprétation, Presses universitaires de Rennes, Rennes.

Lefebvre, F., 2023. Contrôle de gestion et transformation numérique des organisations publiques, Paris, Dunod.

Matell, M.S. et Jacoby, J., 1971. « Is There an Optimal Number of Alternatives for Likert Scale Items ? Effects of Testing Time and Scale Properties », Journal of Applied Psychology, Washington D.C., vol. 56, n° 6, décembre, pp. 506–509.

Mikes, A. et Kaplan, R., 2015. « When one size doesn't fit all : Evolving directions in the research and practice of enterprise risk management », Journal of Applied Corporate Finance, New York, vol. 27, n° 1, p. 37–52.

Mikes, A. et Kaplan, R.S., 2015. « Risk management in the public sector : Evidence from European tax administrations », Harvard Business School Working Paper, Boston, n° 15-100, pp. 1–74.

Moisdon, J.-C., 2022. Le pilotage des organisations : controverses et pratiques, Presses des Mines, Paris.

Moore, M., Prichard, W. et Fjeldstad, O.-H., 2018. Taxing Africa : Coercion, Reform and Development, Zed Books, Londres.

Mungai, P. et Otieno, S., 2023. « Machine Learning for Fraud Risk Detection in E-Governance Systems », African Journal of Information Systems, Nairobi, vol. 15, n° 1, janvier, pp. 88–105.

Nahapiet, J. et Ghoshal, S., 1998. Social Capital, Intellectual Capital, and the Organizational Advantage, Academy of Management Review, New York, vol. 23, n°2, avril, pp. 242–266.

Nahapiet, J. et Ghoshal, S., 1998. Social Capital, Intellectual Capital, and the Organizational Advantage, Academy of Management Review, New York, Vol. 23, n°2, pp. 242–266.

OCDE, 2021. Lutter contre la fraude et l'évasion fiscales à l'ère numérique, Paris, p. 17.

OCDE, 2023. Perspectives fiscales en Afrique 2023, Paris, p. 14.

OECD, 2017. « Technology tools to tackle tax evasion and tax fraud », OECD Taxation Working Papers, Paris, n°32, novembre, pp. 1–42.

OECD, 2019. « Tax Administration 2019 : Comparative Information on OECD and other Advanced and Emerging Economies », OECD Publishing, Paris, septembre, pp. 140–165.

OECD, 2022. « Digital Transformation Maturity Model for Tax Administrations », OECD Publishing, Paris, février, pp. 1–59.

Orlikowski, W. J., 2020. « Digital work : A research agenda », Information Systems Research, Boston, vol. 31, n°4, décembre, pp. 1147-1160.

Pasquale, F., 2015. « The black box society : The secret algorithms that control money and information », Harvard University Press, Cambridge, janvier, pp. 17–35.

Patton, M.Q., 2015. Qualitative Research et Evaluation Methods, Thousand Oaks : SAGE Publications, 4e édition.

Payne, S.C., 2014. Information Security Governance Simplified, CRC Press, Boca Raton, 348 p.

Power, M., 1997. The Audit Society : Rituals of Verification, Oxford University Press, Oxford.

Power, M., 2007. Organized Uncertainty : Designing a World of Risk Management, Oxford University Press, Oxford.

Power, M., 2013. The Risk Management of Everything : Rethinking the Politics of Uncertainty, Londres, Demos.

Putnam, R. D., 2000. Bowling Alone : The Collapse and Revival of American Community, Simon et Schuster, New York.

Putnam, R. D., 2020. The Upswing : How America Came Together a Century Ago and How We Can Do It Again, New York, Simon et Schuster.

Putnam, R.D., 2000. Bowling Alone : The Collapse and Revival of American Community, Simon et Schuster, New York, 541 p.

Quattrone, P., 2016. « Management accounting goes digital : Will the move make it wiser ? »,

Management Accounting Research, Londres, vol. 31, mars, pp. 118–122.

Reinhold, S. (2007). Separation of Duties in Information Systems Security : Analysis of the Theory and Practice. Munich : GRIN Verlag.

Reinhold, S., 2007. Effective Segregation of Duties : Design and Analysis, Springer, Berlin, 176 p.

Revilla, M.A., Saris, W.E. et Krosnick, J.A., 2014. « Choosing the number of categories in agree–disagree scales », Sociological Methods et Research, Thousand Oaks, vol. 43, n° 1, février, pp. 73–97.

Rogers, E. M., 2003. Diffusion of Innovations, 5e éd., Free Press, New York.

Rwanda Revenue Authority, 2020. Annual Report 2019–2020, Kigali, p. 7.

Rwanda Revenue Authority, 2020. Impact of e-Tax System on Revenue Mobilization : A Two-Year Review, Kigali, RRA Publications.

Sandhu, R. et Samarati, P., 1994. Access Control : Principles and Practice, IEEE Communications Magazine, New York, vol. 32, n°9, septembre, pp. 40–48.

Sandhu, R. S., et Samarati, P. (1994). « Access control : Principles and practice », IEEE Communications Magazine, New York, Vol. 32, n°9, pp. 40–48.

Schein, E. H., 1985. Organizational Culture and Leadership, Jossey-Bass, San Francisco.

Simons, R., 1995. Levers of Control : How Managers Use Innovative Control Systems to Drive Strategic Renewal, Harvard Business School Press, Boston.

Smith, J.K., 2012. Interpretive Inquiry, New York : Routledge.

Tashakkori, A. et Teddlie, C., 2010. SAGE Handbook of Mixed Methods in Social et Behavioral Research, Thousand Oaks : SAGE Publications, 2e édition.

Tazi, S., 2022. La gouvernance fiscale à l'épreuve de la digitalisation en Afrique francophone, Presses de l'Université de Rabat.

Torgler, B., 2011. « Tax morale and compliance : Review of evidence and case studies for Europe », Policy Research Working Paper, Washington, D.C., n° 5922, p. 1–50.

Vaessen, P., Decrop, J. et De Beer, P., 2022. « Algorithmic Governance and the Risk of Regulatory Capture in the Public Sector », Government Information Quarterly, Amsterdam, vol. 39, n°2, juin, pp. 1-11.

Vasarhelyi, M. A., et Halper, F. B. (1991). « The continuous audit of online systems », Auditing : A Journal of Practice et Theory, Sarasota, Vol. 10, n°1, pp. 110–125.

Vasarhelyi, M. A., Kogan, A. et Tuttle, B., 2015. « Big Data in Accounting : An Overview », Accounting Horizons, Sarasota, vol. 29, n° 2, p. 381–396.

Vasarhelyi, M. A., Kogan, A. et Tuttle, B., 2015. « Big Data in Accounting : An Overview », Accounting Horizons, Sarasota, vol. 29, n°2, juin, pp. 381–396.

Vasarhelyi, M.A., Kogan, A. et Tuttle, B., 2015. « Big data in accounting : An overview », Accounting Horizons, Sarasota, vol. 29, n°2, juin, pp. 381–396.

Weill, P. et Ross, J.W., 2005. IT Governance : How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, Boston, 320 p.

Wenzel, M., Krause, R. et Diederich, S., 2020. « Automation and transparency in public sector decision-making : A critical perspective », Public Administration Review, Washington D.C., vol. 80, n°6, novembre, pp. 1072–1084.

Whitman, M.E. et Mattord, H.J., 2010. « Principles of Information Security », Information Systems Security Journal, Boston, vol. 14, n°4, décembre, pp. 25–34.

Whittington, R. et Pany, K., 2016. Principles of Auditing and Other Assurance Services, McGraw-Hill Education, New York, 20e éd., 832 p.

Whittington, R., et Pany, K. (2016). Principles of Auditing and Other Assurance Services. New York : McGraw-Hill Education.

Wolfe, D. T. et Hermanson, D. R., 2004. « The Fraud Diamond : Considering the Four Elements of Fraud », CPA Journal, New York, décembre, pp. 38-42.

Zheng, J., Li, Y., et Wang, Q., 2022. « AI-based Risk Assessment in Digital Tax Environments », International Journal of Accounting Information Systems, Amsterdam, vol. 45, octobre, pp. 100–121.