Les Dynamiques de Collaboration dans la Lutte Contre la Fraude : Une Approche Intégrée entre les fonctions d'Audit Interne, de Gestion des Risques et d'Audit Externe

Auteur : Allam, Zakaria
Promoteur(s) : Essaheli, Hanine
Faculté : HEC-Ecole de gestion de l'Université de Liège
Diplôme : Master de spécialisation en gestion des risques financiers
Année académique : 2024-2025
URI/URL : http://hdl.handle.net/2268.2/25025

Les Dynamiques de Collaboration dans la Lutte Contre la Fraude : Une Approche Intégrée entre les fonctions d'Audit Interne, de Gestion des Risques et d'Audit Externe.

Jury :

Promoteur : M. ESSAHELI Hanine

Lecteurs : Mme RICHELLE Isabelle

Mémoire présenté par : **ALLAM Zakaria** En vue de l'obtention du diplôme Master de spécialisation en Gestion des Risques Financiers, Année académique 2024/2025

Remerciement

Je tiens à exprimer ma profonde gratitude à toutes les personnes et institutions qui ont, de près ou de loin, contribué à la réalisation de ce mémoire.

Je remercie tout particulièrement mon promoteur, Monsieur Essaheli Hanine, pour son accompagnement bienveillant, sa disponibilité et la qualité de ses conseils, ainsi que Madame Isabelle Richelle, pour son regard attentif et constructif en tant que lectrice.

Ma reconnaissance s'étend également aux professionnels ayant accepté de participer aux entretiens, dont les témoignages ont enrichi la dimension empirique de ce travail.

Je remercie l'ensemble du corps professoral et administratif de HEC Liège pour la qualité de l'enseignement et le soutien constant tout au long de mon parcours.

Enfin, j'exprime toute ma gratitude à ma famille et mes proches, pour leur patience, leurs encouragements et leur soutien indéfectible. Leur présence, même à distance, a été ma plus grande source de motivation.

Abstract

This thesis explores the collaborative dynamics between internal audit, risk management, and external audit in combating fraud through an integrated approach. Based on semi-structured interviews with professionals, the study examines how these three functions interact despite distinct mandates and constraints. Findings reveal a significant gap between theoretical frameworks and actual practices. While internal audit and risk management form the core of prevention and detection mechanisms, external audit contributes indirectly by enhancing overall credibility. The main challenge lies in balancing independence with effective collaboration. Key obstacles include role confusion, lack of formal coordination, organizational silos, and limited information sharing. Regular, high-quality communication particularly direct, face-to-face interaction emerges as the cornerstone of successful collaboration. The study proposes four recommendations: clarify complementary roles, establish coordination mechanisms, foster a culture of cooperation while preserving independence, and combine technology with human interaction.

Keywords: Fraud, Internal Fraud, External Fraud, Collaboration, Internal Audit, External Audit, Risk Management, Integrated Approach, ISA 240

Table des Matières

Liste des Abrévéation

Abréviation	Signification
ACFE	Association of Certified Fraud Examiners
CFO	Chief Financial Officer
CNCC	Compagnie Nationale des Commissaires aux Comptes
COSO	Committee of Sponsoring Organizations of the Treadway Commission
COSO ERM	Enterprise Risk Management (Cadre du COSO)
CPRO	Contrôle Permanent et Risque Opérationnel
CRF	Cellule de Renseignement Financier
CSOEC	Conseil Supérieur de l'Ordre des Experts-Comptables
CSSF	Commission de Surveillance du Secteur Financier
FSMA	Financial Services and Markets Authority
IA	Intelligence Artificielle
IAASB	International Auditing and Assurance Standards Board
IFAC	International Federation of Accountants
IIA	The Institute of Internal Auditors
IRE	Institut des Réviseurs d'Entreprises
ISA	International Standards on Auditing
JET	Journal Entries Testing
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MOD	Management Override of Control
OLAF	Office Européen de Lutte Antifraude
REA	Réviseur d'Entreprise Agréé
RO	Risque Opérationnel
TPM	Team Planning Meeting
TVA	Taxe sur la Valeur Ajoutée

1 Chapitre I : Introduction

1.1 Contexte : Enjeux de la fraude et rôle des fonctions clés :

Le monde de l'entreprise a profondément changé. Avec la digitalisation et la mondialisation, les opportunités se sont multipliées, mais les risques aussi. Parmi eux, la fraude est devenue une préoccupation majeure et constante. Ce n'est plus un simple problème technique ; c'est une menace qui peut prendre des formes très variées, du détournement de fonds par un employé à la cyberattaque sophistiquée, et qui peut toucher n'importe quelle organisation.

Ce qui rend la fraude si dangereuse, ce n'est pas seulement l'argent perdu. C'est tout ce qu'elle détruit autour : la réputation d'une entreprise, la confiance des investisseurs et des clients, et même le climat de travail en interne. Face à un tel enjeu, les entreprises ne peuvent plus se contenter de réagir après coup. Elles ont dû mettre en place de véritables lignes de défense.

Aujourd'hui, cette défense s'articule principalement autour de trois fonctions clés :

- L'**audit interne**, qui agit depuis l'intérieur pour s'assurer que les systèmes de contrôle de l'entreprise sont solides et fonctionnent correctement.
- La **gestion des risques**, dont le travail est d'anticiper les menaces, y compris la fraude, et de dessiner la stratégie pour les maîtriser.
- L'**audit externe**, ou le réviseur d'entreprises, qui, en certifiant les comptes, apporte un regard extérieur et indépendant, essentiel pour garantir la fiabilité de l'information financière, avec des responsabilités spécifiques concernant la fraude définie par la norme ISA 240.

Pourtant, et c'est là tout le point de départ de ce mémoire, la simple existence de ces trois fonctions ne semble pas suffire. Les scandales financiers continuent de défrayer la chronique, montrant que des failles subsistent. La question n'est donc plus seulement de savoir si chaque métier effectue bien son travail dans son coin, mais de comprendre comment ils pourraient mieux le faire *ensemble*. C'est dans les "angles morts" entre ces fonctions, dans les manques de communication ou de coordination, que la fraude trouve souvent un espace pour se développer.

Ce travail de recherche se propose donc d'explorer précisément cette zone grise, à l'intersection des mandats. L'objectif est de comprendre comment dépasser une simple juxtaposition de compétences pour construire une véritable synergie, créatrice d'un dispositif de défense plus résilient face à la fraude.

1.2 Problématique et justification du sujet :

L'architecture de contrôle des entreprises modernes s'appuie sur un ensemble de fonctions bien établies. La présence de l'audit interne, de la gestion des risques et de l'audit externe constitue un docle la maîtrise des risques. En théorie, cette organisation devrait offrir une protection solide contre les menaces, et notamment contre la fraude.

Cependant, mon intérêt pour ce sujet est né d'un constat simple, issu de l'expérience professionnelle et d'échanges avec de futurs praticiens : sur le terrain, une confusion persiste souvent quant aux rôles et aux périmètres exacts de chacun. Cette ambiguïté n'est pas sans conséquence. Elle peut conduire à une duplication des efforts, mais aussi, et c'est plus préoccupant, à des zones de risque moins bien couvertes, où chaque fonction suppose que l'autre intervient.

Face à ce défi, la justification de notre travail se déploie en deux temps, répondant à un double besoin de clarification et de collaboration.

Le premier temps, d'ordre pédagogique et managérial, est celui de la clarification. Il semble essentiel de revenir aux fondamentaux pour délimiter clairement les mandats et les responsabilités de chaque fonction, en s'appuyant sur les référentiels professionnels (IIA, ISA, COSO). L'objectif est de rendre le dispositif de contrôle plus lisible pour tous les acteurs, afin que chacun puisse mieux se positionner et interagir.

Le second temps, d'ordre stratégique et académique, est celui de la collaboration. Car une fois les rôles bien compris, la question de leur interaction devient centrale. Ce mémoire vise à explorer comment, au-delà d'une simple juxtaposition de compétences, une coopération structurée peut devenir un véritable levier d'efficacité. Il s'agit de comprendre comment articuler ces forces pour transformer un ensemble de fonctions en un système de défense plus intégré et plus performant face au risque de fraude.

1.3 Objectifs et questions de recherche :

L'objectif principal de ce travail est d'analyser les dynamiques de collaboration entre l'audit interne, la gestion des risques et l'audit externe, afin de proposer un modèle de coopération plus efficace et intégré dans la lutte contre la fraude. Il s'agit de dépasser une vision en silos pour comprendre comment la synergie entre ces trois fonctions peut renforcer la résilience globale de l'organisation.

Pour atteindre cet objectif, notre recherche sera guidée par une question de recherche principale :

Comment l'audit interne, la gestion des risques et l'audit externe peuvent-ils collaborer plus efficacement pour prévenir, détecter et répondre au risque de fraude ?

Cette question centrale se décline en plusieurs sous-questions qui structureront notre analyse :

- **Quelles sont les responsabilités spécifiques et les limites de chaque fonction ?** Avant d'étudier la collaboration, il est essentiel de clarifier le rôle de chacun. Quelles sont les obligations de l'audit interne selon les normes IIA ? Quel est le périmètre exact de l'auditeur externe selon la norme ISA 240 ? Comment la fonction de gestion des risques s'articule-t-elle avec les deux autres ?
- **Quels sont les mécanismes de collaboration et les freins observés sur le terrain ?** Cette question vise à identifier les pratiques concrètes. Comment l'information est-elle partagée ? Existe-t-il des instances de coordination formelles ? À l'inverse, quels sont les obstacles culturels, organisationnels ou liés à la confidentialité et l'indépendance qui entravent une coopération efficace ?
- **Comment le rôle complémentaire de l'audit externe peut-il être optimisé ?** L'auditeur externe a un mandat spécifique. Comment peut-il, tout en préservant son indépendance, s'appuyer sur les travaux des fonctions internes et, en retour, enrichir leur propre évaluation du risque de fraude ?
- **Quel est l'impact des nouvelles technologies sur cette collaboration ?** Les outils comme l'analyse de données ou l'intelligence artificielle sont souvent présentés comme des solutions techniques. Comment peuvent-ils également servir de catalyseur pour une meilleure coopération interservices, en créant un langage et des plateformes de travail communs ?

En répondant à ces questions, ce mémoire ambitionne de formuler des recommandations opérationnelles pour aider les organisations à construire un dispositif anti-fraude véritablement intégré, où la collaboration n'est plus une option, mais le cœur de la stratégie de défense.

1.4 Méthodologie utilisée :

La méthodologie adoptée dans ce travail repose sur une approche qualitative, particulièrement adaptée à l'étude des dynamiques de collaboration entre différentes fonctions organisationnelles. Ce choix se justifie par la volonté de comprendre en profondeur les perceptions, les pratiques et les interactions des acteurs impliqués dans la lutte contre la fraude, plutôt que de se limiter à une analyse strictement quantitative.

Deux principaux volets méthodologiques ont été retenus :

- **Recherches académiques et analyse documentaire**

Une revue approfondie de la littérature a été réalisée, s'appuyant sur des **articles scientifiques** ainsi que sur les **cadres théoriques et normatifs** existants (COSO ERM, Model, normes ISA et IIA, etc.).

Cette analyse documentaire s'appuie également sur les **normes professionnelles** (notamment l'ISA 240 pour l'audit externe et les Standards de l'IIA 2025 pour l'audit interne)

et les **rapports d'organisations spécialisées** telles que l'Association of Certified Fraud Examiners (ACFE) et l'Office européen de lutte antifraude (OLAF).

L'objectif est de fournir un **cadre théorique solide** pour analyser les résultats empiriques et formuler des recommandations alignées sur les meilleures pratiques internationales.

- **Entretiens semi-directifs avec des professionnels**

Afin de compléter l'approche théorique, des **entretiens semi-directifs** ont été menés auprès de professionnels évoluant dans les trois métiers étudiés : auditeurs internes, auditeurs externes (Managers, Senior Managers et Réviseurs d'entreprises) et gestionnaires de risques.

Les entretiens ont été conçus pour recueillir des **témoignages détaillés** sur les pratiques existantes, les défis rencontrés et les pistes d'amélioration en matière de collaboration dans la lutte contre la fraude.

Ce choix méthodologique permet d'obtenir des données, révélant la réalité du terrain et les attentes des praticiens, tout en laissant la possibilité d'approfondir certains points soulevés spontanément par les répondants.

En combinant ces deux volets, cette méthodologie vise à croiser les approches théoriques et pratiques, afin de dégager des conclusions et recommandations à la fois robustes sur le plan académique et pertinentes pour le monde professionnel.

2 Chapitre II : Cadre Théorique Revue de la littérature

2.1 Introduction :

Cette deuxième partie constitue le socle théorique de notre mémoire et répond à un double objectif : clarifier les concepts fondamentaux qui sous-tendent notre analyse et établir un état des lieux de la recherche existante sur la collaboration dans la lutte contre la fraude. Pour analyser avec pertinence les dynamiques d'interaction entre l'audit interne, la gestion des risques et l'audit externe, il est indispensable de maîtriser les concepts, les cadres théoriques et les débats qui structurent ce domaine de recherche.

Notre revue de la littérature suivra une progression logique qui nous mènera de la compréhension du phénomène à l'analyse de sa gestion collaborative. Nous commencerons par définir et comprendre la fraude dans toute sa complexité : ses mécanismes, ses typologies et les modèles théoriques qui permettent de l'appréhender, notamment le célèbre **"triangle de la fraude".** Cette base conceptuelle nous permettra ensuite de délimiter avec précision les rôles et responsabilités de chacune des trois fonctions étudiées. Cette clarification est d'autant plus nécessaire que notre problématique part du constat d'une confusion persistante sur le terrain quant aux périmètres d'intervention de chacun. Enfin, nous explorerons les outils, méthodes et dynamiques de collaboration existants, en analysant à la fois les bonnes pratiques identifiées dans la littérature et les défis qui entravent une coopération efficace.

Pour construire cette analyse, nous mobiliserons plusieurs sources de connaissances complémentaires. Nous nous appuierons principalement sur la recherche académique, qui constitue le cœur de notre démarche scientifique. Les articles de recherche nous permettront de comprendre les débats théoriques actuels, d'analyser les perceptions et les comportements des auditeurs face au risque de fraude, et d'identifier les facteurs qui influencent l'efficacité de leur action. Cette base académique sera enrichie par l'analyse des cadres normatifs (Normes IIA pour l'audit interne, ISA 240 pour l'audit externe, référentiels COSO) qui définissent les obligations professionnelles et structurent la pratique quotidienne de ces métiers. Enfin, nous intégrerons les données et perspectives issues des rapports professionnels (notamment ceux de l'ACFE) pour ancrer notre propos dans les réalités du terrain et les tendances actuelles de la fraude.

L'ambition de cette démarche est de construire un cadre d'analyse robuste et nuancé, qui nous servira de grille de lecture pour interpréter les données empiriques collectées lors de nos entretiens. Cette revue de littérature nous permettra également d'identifier les lacunes dans la recherche existante et de positionner notre contribution dans le débat académique. En effet, si la littérature a largement étudié chaque fonction de manière isolée, peu de travaux se sont penchés sur les dynamiques concrètes de leur collaboration, particulièrement dans le contexte spécifique de la lutte contre la fraude. C'est précisément cette lacune que notre recherche empirique ambitionne de combler.

2.2 Concepts clés de la lutte contre la fraude

2.2.1 Définition de la fraude et typologie :

La fraude, en tant que concept juridique et managérial, nécessite une définition précise pour délimiter le périmètre de notre analyse. Plusieurs organismes de référence ont proposé des définitions qui, bien que convergentes, apportent chacune des nuances importantes.

Selon la norme internationale d'audit ISA 240, la fraude se définit comme "un acte intentionnel commis par une ou plusieurs personnes faisant partie de la direction, de personnes constituant le gouvernement d'entreprise, d'employés ou de tiers, impliquant l'utilisation de tromperies pour obtenir un avantage injuste ou illégal" (ISA 240, par. 11). Cette définition met l'accent sur trois éléments fondamentaux : l'**intentionnalité** de l'acte, la **tromperie** comme moyen d'action, et la recherche d'un **avantage indu**.

L'Association of Certified Fraud Examiners (ACFE), organisation mondiale de référence dans la lutte contre la fraude, propose une approche complémentaire en définissant la fraude comme "l'utilisation de sa profession à des fins d'enrichissement personnel par l'abus délibéré ou la mauvaise utilisation des ressources ou des actifs de l'organisation qui l'emploie". Cette définition de l'ACFE insiste particulièrement sur la dimension professionnelle de la fraude et sur l'abus de confiance qu'elle représente, élargissant ainsi la perspective au-delà des seules considérations comptables pour englober tous les types de détournements organisationnels.

Les normes professionnelles distinguent traditionnellement deux grandes catégories de fraude selon leur nature et leur impact sur l'organisation. La **fraude interne** regroupe les actes commis par les employés, dirigeants ou administrateurs de l'entreprise. Elle englobe notamment les détournements d'actifs, les abus de biens sociaux, les falsifications comptables et les manipulations d'états financiers. À l'inverse, la **fraude externe** émane de parties tierces à l'organisation et comprend les escroqueries, les cyberattaques, les fraudes contractuelles et les fraudes aux marchés publics.

Une troisième catégorie mérite une attention particulière : la **fraude collusive**, qui implique une collaboration entre des acteurs internes et externes à l'organisation. Cette forme de fraude est particulièrement préoccupante car elle combine la connaissance intime des systèmes internes avec des ressources ou des opportunités externes, créant ainsi des schémas sophistiqués et difficiles à détecter.

La recherche académique a également enrichi notre compréhension de la fraude en développant des modèles explicatifs de ses mécanismes. Le plus célèbre d'entre eux, le "triangle de la fraude" développé par Donald Cressey, identifie trois conditions nécessaires à la réalisation d'un acte frauduleux : la **pression** (motivation financière ou personnelle), l'**opportunité** (faille dans les contrôles permettant l'acte), et la **rationalisation** (justification morale que se donne l'auteur). Ce modèle théorique est devenu un référentiel

incontournable pour comprendre les mécanismes psychologiques et organisationnels qui favorisent l'émergence de la fraude (Verwey & Asare, 2021 ; Jizi et al., 2017).

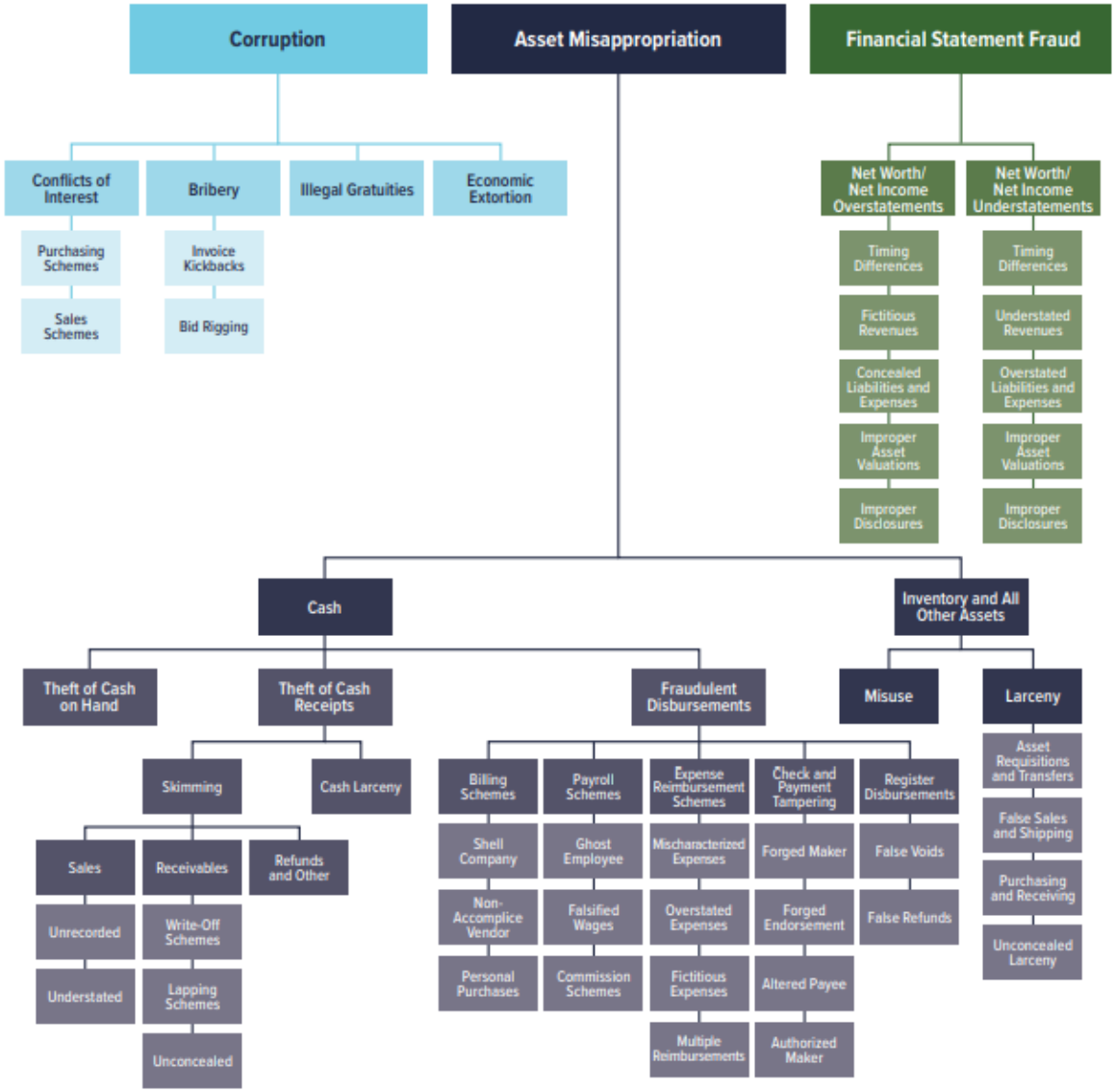

FIGURE 1 : OCCUPATIONAL FRAUD 2024 : A REPORT TO THE NATIONS ACFE, FRAUD TREE

2.2.2 Les étapes clés de la gestion de la fraude

La gestion efficace de la fraude ne se limite pas à sa simple détection après qu'elle ait eu lieu. Elle s'inscrit dans une démarche globale et structurée qui englobe l'ensemble du cycle de vie du risque frauduleux. La recherche académique et les pratiques professionnelles convergent pour identifier quatre étapes fondamentales dans cette approche intégrée.

2.2.2.1 La prévention :

Constitue la première ligne de défense et sans doute la plus efficace. Elle repose sur la mise en place de dispositifs de contrôle interne robustes, le développement d'une culture éthique forte au sein de l'organisation, et l'établissement de politiques antifraude claires et communiquées. Cette approche préventive s'appuie sur une compréhension fine du triangle

de la fraude : en réduisant les opportunités par des contrôles appropriés et en agissant sur les pressions par une culture organisationnelle saine, les entreprises peuvent significativement diminuer le risque de survenance d'actes frauduleux. Comme le démontrent Mangala et Kumari (2017) dans leur analyse des perceptions des auditeurs, la gouvernance d'entreprise, incluant un comité d'audit indépendant et un code de conduite, est perçue comme le facteur le plus efficace dans la lutte contre la fraude, devançant même les outils technologiques et les procédures d'audit.

2.2.2.2 La détection :

Représente la deuxième étape cruciale lorsque les mesures préventives s'avèrent insuffisantes. Elle mobilise un arsenal d'outils et de techniques : audits ciblés, analyses de données avancées (data Analytics), mécanismes de dénonciation (whistleblowing), et surveillance continue des transactions. Selon Drogalas et ses collègues (2017), l'efficacité de la détection par les auditeurs internes dépend largement de trois facteurs statistiquement significatifs : l'efficacité globale de la fonction d'audit interne, le sentiment de responsabilité de l'auditeur interne, et sa formation spécialisée sur les schémas de fraude spécifiques à son secteur d'activité. Cette conclusion est renforcée par les travaux de Wahidahwati et Asyik (2022), qui identifient quatre déterminants clés de la capacité des **auditeurs internes** à détecter la fraude : leur expérience professionnelle, leur éthique personnelle, leur scepticisme professionnel, et leur type de personnalité.

2.2.2.3 L'investigation :

Intervient dès qu'une suspicion de fraude est identifiée. Cette phase requiert des compétences spécialisées en audit forensique, la conduite d'enquêtes internes rigoureuses, et souvent une coopération avec les autorités compétentes. L'objectif est double : établir les faits avec précision et préserver les preuves nécessaires aux éventuelles poursuites. Comme le soulignent Demirović et ses collègues (2021), le rôle de l'**auditeur interne** dans cette phase n'est pas de sanctionner, mais de faire des recommandations au management pour corriger les faiblesses identifiées et éviter la récurrence des incidents.

2.2.2.4 La remédiation :

Vise à tirer les enseignements de l'incident pour renforcer le dispositif de contrôle. Elle comprend le renforcement des contrôles défaillants, l'application de sanctions appropriées, et une communication transparente auprès des parties prenantes pour restaurer la confiance. Cette étape est essentielle car elle transforme l'incident en opportunité d'apprentissage organisationnel et permet d'adapter les stratégies de prévention aux nouvelles menaces identifiées.

Cette approche en quatre temps illustre parfaitement pourquoi la lutte contre la fraude ne peut être l'apanage d'une seule fonction. Chaque étape mobilise des compétences et des perspectives différentes, justifiant pleinement la nécessité d'une collaboration structurée

2.2.3 Approches intégrées et modèles de gouvernance

La lutte contre la fraude ne peut être efficace si elle est laissée à la seule charge d'une fonction isolée. La complexité du risque de fraude impose une approche structurée et coordonnée, impliquant plusieurs acteurs au sein de l'organisation. Pour organiser cette répartition des rôles, plusieurs cadres de gouvernance ont été développés. Deux d'entre eux sont particulièrement pertinents pour notre étude : le modèle des Trois Lignes de l'IIA, qui clarifie les responsabilités, et le référentiel COSO ERM, qui intègre la gestion du risque de fraude dans la stratégie globale de l'entreprise.

2.2.3.1 Le Modèle des Trois Lignes (Three Lines Model) de l'IIA

Proposé par l'Institute of Internal Auditors (IIA) et mis à jour en 2020, le "Three Lines Model" est un cadre de référence internationalement reconnu pour structurer la gouvernance et la gestion des risques. Il clarifie les rôles et les responsabilités des différentes parties prenantes et favorise une communication et une coordination efficaces. Son application à la lutte contre la fraude est particulièrement éclairante.

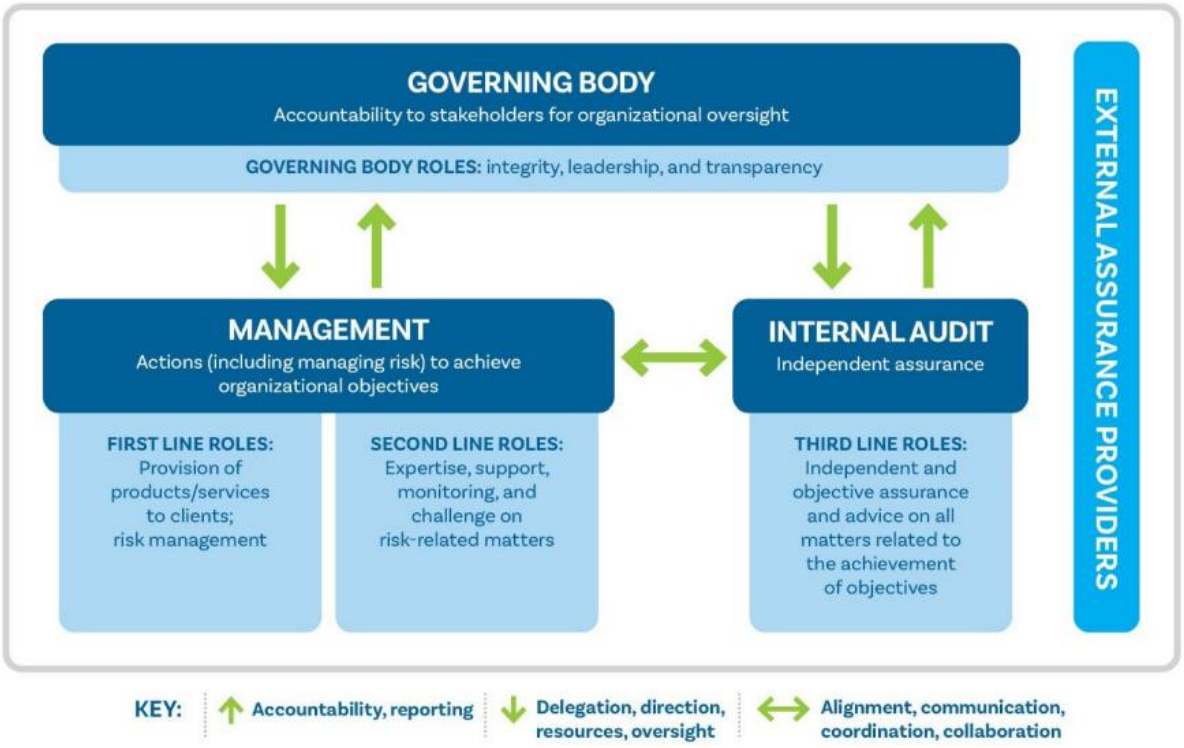

FIGURE 2 : THE IIA'S THREE LINES MODEL AN UPDATE OF THE THREE LINES OF DEFENSE

2.2.3.1.1 La Première Ligne : Le Management Opérationnel

La première ligne est constituée des managers opérationnels et de leurs équipes. Ce sont eux qui "possèdent" les risques et sont responsables de leur gestion au quotidien. Dans la lutte contre la fraude, leur rôle est avant tout préventif. Ils doivent mettre en œuvre les politiques et les procédures de contrôle interne définies par l'organisation, superviser leurs équipes et s'assurer que les opérations se déroulent de manière conforme. Ils sont en

première position pour détecter les comportements anormaux et créer un environnement de travail éthique. Leur responsabilité est directe et permanente.

2.2.3.1.2 La Deuxième Ligne : Les Fonctions de Supervision et d'Expertise

La deuxième ligne regroupe les fonctions qui apportent une expertise et une supervision en matière de gestion des risques et de conformité. C'est ici que se situe principalement la fonction de gestion des risques (Risk Management). Son rôle n'est pas de gérer les risques à la place de la première ligne, mais de lui fournir les outils, les méthodologies et l'expertise nécessaires. Concernant la fraude, la deuxième ligne aide à développer le cadre de gestion du risque de fraude, facilite l'identification et l'évaluation des scénarios de fraude potentiels, et s'assure que les contrôles mis en place par la première ligne sont adéquatement conçus.

2.2.3.1.3 La Troisième Ligne : L'Assurance Indépendante

La troisième ligne est incarnée par l'audit interne. Son rôle est de fournir une assurance indépendante et objective au Conseil et à la direction générale sur l'efficacité de la gouvernance, de la gestion des risques et du contrôle interne. L'audit interne ne participe pas directement à la mise en place des contrôles (pour ne pas compromettre son objectivité), mais il évalue leur conception et leur efficacité opérationnelle. Comme l'exige la Norme IIA 9.5, l'audit interne se coordonne avec les deux premières lignes pour éviter les redondances et s'assurer que tous les risques significatifs, y compris la fraude, sont correctement couverts. Il agit comme un "filet de sécurité" qui vérifie que l'ensemble du dispositif fonctionne comme prévu.

L'audit externe, bien que ne faisant pas partie intégrante du modèle interne de l'organisation, interagit principalement avec la troisième ligne et le gouvernement d'entreprise (le Conseil). Il s'appuie sur les travaux de l'audit interne (après évaluation de sa compétence et de son objectivité) et utilise les informations des trois lignes pour planifier et réaliser sa propre mission d'assurance sur les états financiers.

2.2.3.2 Le Référentiel COSO ERM et l'intégration du risque de fraude

Le référentiel "Enterprise Risk Management (ERM) - Integrating with Strategy and Performance" du COSO (2017) offre un cadre pour intégrer la gestion des risques dans la prise de décision stratégique. Bien que plus large que la seule fraude, il fournit une méthodologie essentielle pour s'assurer que le risque de fraude n'est pas traité comme un sujet secondaire.

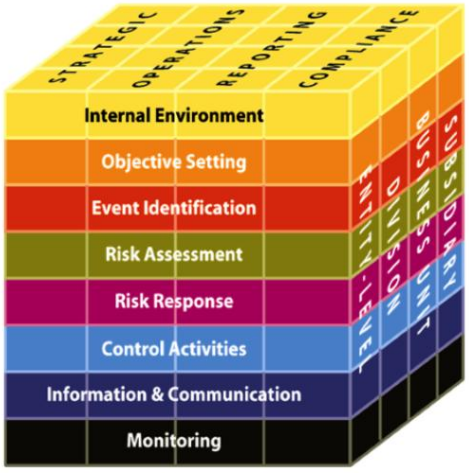

FIGURE 3 : ENTERPRISE RISK MANAGEMENT (ERM) - INTEGRATING WITH STRATEGY AND PERFORMANCE

2.2.3.2.1 Le COSO ERM préconise un processus continu :

Identifier les risques : L'organisation doit identifier de manière proactive les événements potentiels, y compris les schémas de fraude internes et externes, qui pourraient affecter la réalisation de ses objectifs.

Évaluer les risques : Une fois identifiés, les risques de fraude doivent être évalués selon leur probabilité d'occurrence et leur impact potentiel (financier, réputationnel, etc.). Cette évaluation permet de créer une cartographie des risques qui hiérarchise les menaces les plus critiques. C'est ici que la méthode de décomposition (Likelihood x Magnitude) trouve son application pratique.

Répondre aux risques : En fonction de sa position sur la cartographie et de l'appétence pour le risque de l'entreprise, une réponse est définie pour chaque risque de fraude : l'accepter, le réduire (par des contrôles), le partager (par une assurance) ou l'éviter.

Surveiller les risques : Le dispositif doit être surveillé en permanence pour s'assurer de son efficacité et l'ajuster en fonction de l'évolution de l'environnement.

L'intégration de ces deux modèles est fondamentale. Le COSO ERM fournit le "quoi" et le "pourquoi" (identifier et évaluer le risque de fraude en lien avec la stratégie), tandis que le Modèle des Trois Lignes fournit le "qui" (définir clairement les responsabilités de chaque acteur dans ce processus). Une collaboration efficace entre l'audit interne, la gestion des risques et l'audit externe ne peut donc s'envisager qu'à travers le prisme de ces cadres de gouvernance qui organisent leurs interactions et légitiment leurs mandats respectifs.

2.3 Rôles et responsabilités dans la lutte contre la fraude

2.3.1 L'audit interne : garant du contrôle et de l'amélioration continue

Au sein de l'architecture de gouvernance d'une organisation, l'audit interne occupe une position unique. Il est positionné comme la troisième ligne du "Three Lines Model", chargé

de fournir une assurance indépendante et objective au Conseil et à la direction générale sur l'efficacité de l'ensemble des processus de gouvernance, de gestion des risques et de contrôle. Plusieurs études empiriques confirment que l'audit interne est perçu par les professionnels comme un acteur de premier plan contre la fraude.

2.3.1.1 Mandat et missions selon les Normes IIA

Le rôle de l'audit interne est formellement défini par les Normes Internationales pour la Pratique Professionnelle de l'Audit Interne de l'IIA. La mission fondamentale de l'audit interne est de "renforcer la capacité de l'organisation à créer de la valeur et à œuvrer pour sa protection et sa pérennité". Pour ce faire, il doit évaluer et contribuer à l'amélioration des processus de gouvernance, de gestion des risques et de contrôle.

Concernant spécifiquement la fraude, les normes sont explicites. Le plan d'audit interne doit être fondé sur une évaluation des risques de l'organisation et doit tenir compte du risque de fraude ***(Norme 9.4).*** Cela signifie que la fraude n'est pas un sujet optionnel, mais une composante obligatoire du champ d'intervention de l'audit interne. De plus, lors de la planification de chaque mission, les auditeurs internes doivent évaluer les risques y afférents, en prenant en compte les ***"risques spécifiques liés à la fraude" (Norme 13.2).***

Cette responsabilité est renforcée par l'exigence de scepticisme professionnel ***(Norme 4.3),*** qui demande aux auditeurs internes d'évaluer de manière critique la fiabilité des informations et de ne pas se fier aveuglément aux déclarations de la direction.

2.3.1.2 Rôle dans la prévention et la détection de la fraude

Le rôle de l'audit interne couvre l'ensemble du cycle de gestion de la fraude, avec une implication particulièrement forte dans les phases de prévention et de détection.

Rôle dans la prévention : L'action préventive de l'audit interne est indirecte mais fondamentale. Il ne conçoit pas les contrôles lui-même (pour préserver son objectivité), mais il en évalue la conception et l'efficacité. En identifiant les faiblesses du contrôle interne, les "opportunités" dans le triangle de la fraude, et en recommandant leur renforcement, il contribue directement à réduire la probabilité d'occurrence de la fraude. Des recherches ont montré qu'une fonction d'audit interne jugée efficace est positivement et significativement corrélée à une meilleure détection de la fraude, notamment parce qu'elle assure que "la structure du système de contrôle prévient les erreurs".

Rôle dans la détection : L'audit interne est un acteur majeur de la détection. Les revues ciblées, planifiées sur la base de l'évaluation des risques, permettent d'examiner en profondeur les zones les plus exposées. De plus, l'audit interne est souvent le récepteur naturel des alertes issues des mécanismes de dénonciation (whistleblowing). En cas de soupçon, il est le mieux placé pour mener ou superviser les investigations internes initiales, grâce à sa connaissance de l'organisation et à son accès illimité aux informations, aux personnes et aux biens, tel que défini dans sa charte **(Norme 6.1).**

2.3.1.3 Exemples de pratiques et contributions concrètes

La contribution de l'audit interne se matérialise par des pratiques concrètes, dont l'efficacité est corroborée par la recherche.

Évaluation des programmes anti-fraude : L'audit interne évalue l'ensemble du dispositif, y compris l'existence et l'application d'un code de conduite, l'efficacité des formations anti-fraude pour les employés, ou encore la robustesse des contrôles informatiques (pare-feux, cryptage, etc.), qui sont perçus par les auditeurs comme des outils très efficaces.

Gestion des alertes internes : Il s'assure que le processus de whistleblowing est fonctionnel, confidentiel et que les alertes sont traitées de manière appropriée.

Audits de conformité : Il vérifie le respect des lois et règlements, ce qui permet de détecter des actes illégaux qui peuvent être liés à des schémas de fraude.

Analyse de données (Data Analytics) : L'utilisation d'outils d'analyse de données permet à l'audit interne de tester des populations entières de transactions pour identifier des anomalies, des tendances suspectes ou des violations de contrôles, ce qui en fait un outil de détection de plus en plus puissant.

En conclusion, les normes professionnelles et la recherche académique convergent pour positionner l'audit interne comme un pilier central et indispensable de la lutte contre la fraude. Son efficacité dépend cependant de facteurs clés tels que son indépendance, la compétence et la formation de ses équipes, et le soutien qu'il reçoit de la direction et du Conseil.

2.3.2 La gestion des risques : pilier stratégique de la résilience organisationnelle

L'architecture de défense des entreprises contre la fraude s'est progressivement structurée autour de modèles intégrés qui dépassent une vision cloisonnée des responsabilités. Ces cadres conceptuels visent à optimiser la coordination entre les différentes fonctions de contrôle pour créer une synergie dans la lutte contre la fraude.

2.3.2.1 Cadre COSO ERM et intégration des risques de fraude dans la cartographie des risques

Le référentiel COSO Enterprise Risk Management (2017) propose une approche systémique de la gestion des risques qui intègre explicitement le risque de fraude dans la cartographie globale des menaces organisationnelles. Cette intégration permet de dépasser une vision isolée de la fraude pour la considérer comme une composante transversale susceptible d'affecter l'ensemble des processus de l'entreprise.

L'intégration du risque de fraude dans le cadre COSO ERM se traduit par plusieurs dimensions complémentaires. La dimension stratégique évalue l'impact potentiel de la fraude sur les objectifs de l'organisation et sa capacité à créer de la valeur. La dimension opérationnelle identifie les processus les plus exposés et définit les contrôles nécessaires

pour maîtriser ces expositions. Enfin, la dimension de gouvernance assure une remontée d'information structurée vers les instances dirigeantes.

Cette approche intégrée révèle les corrélations entre le risque de fraude et d'autres risques organisationnels, permettant une allocation plus rationnelle des ressources et une gestion plus efficace des interdépendances. Comme le soulignent Jizi et ses collègues (2017), cette vision systémique est essentielle car elle reconnaît que la fraude ne peut être efficacement combattue par les seuls mécanismes de contrôle technique, mais nécessite une approche qui intègre la culture organisationnelle et l'environnement de contrôle dans leur globalité.

2.3.2.2 Rôle des gestionnaires de risques : identification des expositions, quantification des impacts, mise en place de plans d'atténuation

Les gestionnaires de risques occupent une position stratégique dans ce dispositif intégré, agissant comme la deuxième ligne de défense selon le modèle des trois lignes. Leur mission se décline en trois volets complémentaires qui s'articulent de manière séquentielle.

L'identification des expositions constitue le premier volet de leur mission. Il s'agit de cartographier l'ensemble des vulnérabilités de l'organisation face au risque de fraude, en s'appuyant sur une analyse approfondie des processus, des systèmes et de l'environnement de contrôle. Cette identification doit être dynamique et tenir compte des évolutions technologiques, réglementaires et organisationnelles.

La quantification des impacts représente le deuxième volet. Les gestionnaires de risques évaluent les conséquences potentielles de chaque type de fraude, en considérant non seulement les impacts financiers directs, mais aussi les conséquences indirectes sur la réputation, la conformité réglementaire et la continuité des activités.

La mise en place de plans d'atténuation constitue le troisième volet. Il s'agit de concevoir et de coordonner la mise en œuvre de stratégies de traitement du risque, incluant la prévention, la détection, le transfert ou l'acceptation des risques résiduels. Les travaux de Demirović et ses collègues (2021) illustrent l'importance de cette approche méthodologique, en montrant comment l'utilisation d'outils structurés comme les matrices de risques permet aux gestionnaires de risques de prioriser efficacement leurs interventions et d'optimiser l'allocation des ressources de contrôle.

2.3.2.3 Interaction avec le comité d'audit et les instances de gouvernance.

L'efficacité de ces modèles intégrés dépend largement de la qualité des interactions avec les instances de gouvernance, qui définissent l'orientation stratégique et supervisent la mise en œuvre du dispositif de contrôle.

Le comité d'audit constitue l'interface privilégiée entre les fonctions de contrôle et le conseil d'administration. Son rôle dans la lutte contre la fraude est multiple : définition de l'appétit au risque, supervision de l'efficacité du contrôle interne, et coordination entre les différentes

lignes de défense. Cette instance joue également un rôle crucial dans la définition du **"tone at the top"** qui influence l'efficacité de l'ensemble du dispositif.

Les instances de gouvernance (conseil d'administration, comité des risques, comité de direction) contribuent à créer un environnement de contrôle favorable en donnant l'impulsion éthique nécessaire et en allouant les ressources appropriées. Leur engagement visible dans la lutte contre la fraude renforce la crédibilité du dispositif et favorise l'adhésion de l'ensemble des collaborateurs.

Cette interaction se concrétise par des mécanismes de reporting structurés qui permettent une remontée d'information régulière sur l'évolution du risque de fraude, l'efficacité des contrôles et les incidents éventuels. Comme le démontrent Wang et Fargher (2017) dans leur étude expérimentale, cette coordination au niveau de la gouvernance est particulièrement efficace car elle agit comme un mécanisme de renforcement mutuel entre les différentes fonctions de contrôle, créant un effet de synergie qui améliore significativement l'évaluation et la gestion du risque de fraude.

2.3.3 L'audit externe : une contribution complémentaire et indépendante

L'auditeur externe occupe une position unique dans l'écosystème de la lutte contre la fraude. Bien qu'il ne soit pas un membre de la gouvernance interne de l'entreprise, il constitue un maillon externe essentiel dont l'indépendance statutaire et le regard extérieur apportent une valeur distinctive au dispositif de contrôle. Cette section examine en détail les obligations, les contributions et les limites de cette fonction, en s'appuyant sur les dispositions de la norme ISA 240 et les enseignements de la recherche académique.

2.3.3.1 Le cadre normatif de l'ISA 240 : obligations et responsabilités

La norme internationale d'audit ISA 240, intitulée "Les obligations de l'auditeur en matière de fraude lors d'un audit d'états financiers", constitue le socle réglementaire qui définit précisément le périmètre d'intervention de l'auditeur externe. Cette norme établit un équilibre délicat entre les attentes légitimes des parties prenantes et les contraintes pratiques de la mission d'audit.

2.3.3.1.1 L'objectif fondamental et ses limites

Selon l'ISA 240, l'objectif de l'auditeur n'est pas de détecter toutes les fraudes, mais d'obtenir une "assurance raisonnable que les états financiers pris dans leur ensemble ne comportent pas d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs" (ISA 240, par. 5). Cette formulation révèle une limitation fondamentale : l'auditeur externe se concentre sur les fraudes susceptibles d'avoir un impact matériel sur les états financiers, excluant de facto de nombreux types de fraudes internes.

Cette limitation n'est pas fortuite mais découle de la nature même de la mission d'audit externe. Comme l'expliquent Carassus et Cormier (2003) dans leur analyse historique des "Normes et pratiques de l'audit externe légal en matière de prévention et de détection de la fraude", l'évolution de l'audit externe au cours du XXe siècle l'a progressivement éloigné

d'une mission de "détection de fraude" pour l'orienter vers une mission de "certification de l'image fidèle". Cette évolution explique pourquoi les auditeurs externes ne découvrent qu'environ 5% des fraudes selon les statistiques citées par ces auteurs, un taux qui interroge sur l'adéquation entre les attentes du public et la réalité de la mission.

2.3.3.1.2 Le scepticisme professionnel : pierre angulaire de la démarche

L'ISA 240 place le scepticisme professionnel au cœur de la démarche de l'auditeur externe. Le paragraphe 12 de la norme stipule que "l'auditeur doit conserver un esprit critique tout au long de l'audit, en étant conscient de la possibilité que des anomalies significatives puissent résulter de fraudes". Cette exigence va au-delà d'une simple posture intellectuelle ; elle implique une remise en question systématique des déclarations de la direction et une vigilance particulière face aux éléments probants contradictoires.

Cependant, la recherche académique révèle que l'application pratique de ce scepticisme professionnel est plus complexe qu'il n'y paraît. L'étude de Verwey et Asare (2021), intitulée "The Joint Effect of Ethical Idealism and Trait Skepticism on Auditors' Fraud Detection", démontre que l'efficacité du scepticisme professionnel dépend de l'interaction entre deux traits de personnalité de l'auditeur : son scepticisme inné et son idéalisme éthique. Leurs résultats montrent qu'un auditeur externe n'est vraiment efficace dans la détection de fraude que s'il possède à la fois un haut niveau de scepticisme ET un haut niveau d'idéalisme éthique. Cette découverte suggère que le scepticisme professionnel ne peut être réduit à une simple technique d'audit, mais constitue une compétence complexe qui dépend des caractéristiques individuelles de l'auditeur.

2.3.3.1.3 Les procédures spécifiques d'évaluation du risque

L'ISA 240 impose à l'auditeur externe de mettre en œuvre des procédures spécifiques pour identifier et évaluer les risques d'anomalies significatives résultant de fraudes. Ces procédures incluent notamment l'obligation de s'entretenir avec la direction et l'audit interne sur leur propre évaluation du risque de fraude , créant ainsi un point de contact obligatoire avec les fonctions internes.

Cette obligation de coordination trouve un écho particulier dans les travaux de recherche. L'étude d'Al-Dhubaibi et Sharaf-Addin (2022), "An analysis of external and internal auditors' use of ISA 240 red flags: The impact of auditors' estimation of fraud pervasiveness", révèle des différences significatives dans la manière dont les auditeurs internes et externes perçoivent et utilisent les signaux d'alerte de fraude. Leurs résultats montrent que les auditeurs externes accordent plus d'importance aux "red flags" formalisés que les auditeurs internes, mais que cette importance accrue ne se traduit pas nécessairement par une utilisation plus fréquente de ces signaux. Cette découverte souligne l'importance d'une coordination effective entre les deux types d'auditeurs pour optimiser l'utilisation de ces outils de détection.

2.3.3.2 Le rôle indirect mais stratégique de l'auditeur externe

Bien que l'auditeur externe ne soit pas le responsable principal de la prévention et de la détection de la fraude, son intervention revêt une dimension stratégique qui dépasse le cadre strict de la certification des comptes.

2.3.3.2.1 L'identification des anomalies et l'effet dissuasif

L'une des contributions les plus importantes de l'auditeur externe réside dans sa capacité à identifier des anomalies qui pourraient révéler l'existence de fraudes. Cette identification ne résulte pas d'une recherche systématique de la fraude, mais découle de l'application rigoureuse des procédures d'audit visant à détecter les anomalies significatives.

L'effet dissuasif de la présence de l'auditeur externe constitue également une contribution non négligeable. La simple perspective d'un contrôle externe indépendant peut décourager les tentatives de fraude, particulièrement celles qui impliquent une manipulation des états financiers. Cet effet préventif, bien que difficile à quantifier, représente une valeur ajoutée importante du dispositif d'audit externe.

Cependant, la recherche académique nuance cette contribution. L'étude de DeZoort et Harrison (2016), "Understanding Auditors' Sense of Responsibility for Detecting Fraud Within Organizations", utilise le Triangle Model of Responsibility pour analyser les facteurs qui influencent le sentiment de responsabilité des auditeurs face à la fraude. Leurs résultats montrent que les auditeurs externes se sentent plus responsables pour la fraude affectant les états financiers que pour les autres types de fraude (détournement d'actifs, corruption), ce qui peut limiter leur vigilance sur certains types de risques.

2.3.3.2.2 L'évaluation des dispositifs internes et la communication avec la gouvernance

L'auditeur externe joue un rôle crucial dans l'évaluation de l'efficacité des dispositifs de contrôle interne, incluant les mécanismes de prévention et de détection de la fraude. Cette évaluation, bien qu'elle ne constitue pas l'objectif principal de la mission, fournit aux organes de gouvernance une perspective indépendante sur la robustesse du système de contrôle.

L'ISA 240 impose à l'auditeur externe de communiquer aux personnes constituant le gouvernement d'entreprise toute fraude ou suspicion de fraude identifiée (par. 40-41). Cette obligation de communication crée un canal direct entre l'auditeur externe et les instances dirigeantes, renforçant ainsi la gouvernance de l'organisation.

La recherche de Wang et Fargher (2017), "The effects of tone at the top and coordination with external auditors on internal auditors' fraud risk assessments", apporte un éclairage particulièrement intéressant sur cette dimension. Leur étude expérimentale démontre que la coordination entre l'audit interne et l'audit externe améliore l'évaluation du risque de fraude, particulièrement lorsque le "tone at the top" est défaillant. Cette coordination agit comme un mécanisme de compensation qui renforce la résilience globale du dispositif de contrôle.

2.3.3.3 Les limites du mandat et l'expectation gap

L'analyse du rôle de l'auditeur externe ne peut être complète sans une examination approfondie de ses limites intrinsèques et des malentendus qu'elles génèrent.

2.3.3.3.1 Les contraintes structurelles de la mission d'audit

L'auditeur externe opère dans un cadre contraint par plusieurs facteurs qui limitent sa capacité à détecter la fraude. Premièrement, la nature échantillonnée des tests d'audit signifie qu'une fraude peut échapper à la détection si elle n'affecte pas les éléments sélectionnés pour les tests. Deuxièmement, la sophistication croissante des schémas frauduleux, particulièrement ceux impliquant la collusion ou le contournement des contrôles par la direction, peut rendre leur détection extrêmement difficile.

La recherche d'Austin (2022), "Remembering Fraud in the Future: Investigating and Improving Auditors' Attention to Fraud during Audit Testing", révèle une contrainte cognitive supplémentaire. Son étude montre que les auditeurs externes ont du mal à maintenir leur attention sur les indices de fraude pendant les phases de test, car ils sont concentrés sur l'exécution des procédures planifiées. Cette "double tâche" cognitive peut réduire leur capacité à détecter des signaux de fraude inattendus, même lorsqu'ils sont présents.

2.3.3.3.2 L'expectation gap : entre perception et réalité

L'expectation gap, concept central dans la littérature sur l'audit, désigne l'écart entre ce que le public attend de l'auditeur externe et ce que celui-ci peut raisonnablement accomplir dans le cadre de sa mission. Cette divergence est particulièrement marquée en matière de fraude.

L'étude de Jizi, Nehme et ELHout (2017), "Fraud: auditors' responsibility or organisational culture", analyse en profondeur cette problématique. Leurs travaux montrent que les auditeurs externes ont historiquement refusé d'endosser la responsabilité principale de la détection de la fraude, la considérant comme relevant du management. Cette position, bien que justifiée par les contraintes de la mission d'audit, crée une frustration chez les parties prenantes qui attendent une protection plus complète.

Les auteurs soulignent également que cette focalisation sur les responsabilités de l'auditeur externe peut détourner l'attention du véritable enjeu : la création d'une culture organisationnelle résistante à la fraude. Leur analyse suggère que l'efficacité de la lutte contre la fraude dépend moins de l'intensification des contrôles techniques que de l'établissement d'un environnement éthique solide.

2.3.3.3.3 Les biais cognitifs dans l'évaluation des risques

La recherche académique récente a identifié des biais cognitifs qui peuvent affecter l'évaluation des risques de fraude par les auditeurs externes. L'étude de Simon, Smith et Zimbelman (2018), "The Influence of Judgment Decomposition on Auditors' Fraud Risk Assessments: Some Trade-Offs", révèle un paradoxe troublant : la méthode de

décomposition du risque (probabilité × impact) recommandée par les normes peut conduire les auditeurs externes à sous-estimer les risques de fraude les plus graves.

Cette découverte remet en question certaines pratiques d'audit établies et suggère que l'amélioration de l'efficacité de l'audit externe ne passe pas seulement par le renforcement des procédures, mais aussi par une meilleure compréhension des mécanismes cognitifs qui influencent le jugement professionnel.

2.4 Outils, méthodologies et dynamiques de collaboration

Après avoir établi les fondements conceptuels de la fraude et délimité les responsabilités théoriques de chaque fonction, cette troisième partie de notre revue de littérature examine la dimension opérationnelle et collaborative de la lutte contre la fraude. La recherche académique récente a commencé à s'intéresser aux mécanismes concrets d'interaction entre les différentes fonctions de contrôle, révélant à la fois des opportunités de synergie et des défis organisationnels significatifs.

Les travaux existants mettent en évidence une évolution dans la compréhension de l'efficacité anti-fraude : d'une approche centrée sur les compétences individuelles de chaque fonction vers une reconnaissance croissante de l'importance des dynamiques collaboratives. Cette évolution reflète une prise de conscience que l'efficacité du dispositif global dépend autant de la qualité des interactions que de la performance individuelle de chaque composante.

Notre analyse s'articulera autour de quatre dimensions complémentaires. Nous examinerons d'abord les outils et méthodes documentés par la recherche, en analysant leur efficacité perçue et leur utilisation par les différentes fonctions. Nous explorerons ensuite les modèles et pratiques de collaboration identifiés dans la littérature, en nous appuyant sur les études qui ont analysé les facteurs de succès et d'échec de ces interactions. La troisième dimension portera sur l'analyse des obstacles et des défis mis en évidence par la recherche empirique, qui révèlent les tensions inhérentes à la coordination de fonctions aux cultures professionnelles distinctes. Enfin, nous examinerons les perspectives ouvertes par les innovations technologiques, domaine où la recherche commence à documenter les impacts sur la collaboration inter-fonctionnelle.

Cette approche nous permettra de synthétiser les connaissances actuelles et d'identifier les questions qui méritent un approfondissement empirique dans le contexte spécifique de notre étude.

2.4.1 Outils et méthodes existants

L'arsenal des outils et méthodes disponibles pour lutter contre la fraude s'est considérablement enrichi au cours des dernières décennies, évoluant des contrôles manuels traditionnels vers des solutions technologiques sophistiquées. La recherche académique a

progressivement documenté l'efficacité relative de ces différents instruments, révélant des nuances importantes dans leur perception et leur utilisation par les professionnels.

2.4.1.1 Contrôles internes robustes : lignes de défense et matrices de risques

Les contrôles internes constituent le socle fondamental de tout dispositif anti-fraude. Leur organisation selon le modèle des lignes de défense permet une répartition claire des responsabilités et une couverture systématique des risques. Les matrices de risques, outils de cartographie et de priorisation, complètent ce dispositif en permettant une allocation rationnelle des ressources de contrôle.

La recherche de Mangala et Kumari (2017) dans leur étude "Auditors' Perceptions of the Effectiveness of Fraud Prevention and Detection Methods" fournit un éclairage précieux sur l'efficacité perçue de ces outils traditionnels. Leur enquête révèle que la gouvernance d'entreprise, incluant un comité d'audit indépendant et un code de conduite, est perçue comme le facteur le plus efficace dans la lutte contre la fraude, devançant même les outils technologiques avancés. Cette conclusion souligne l'importance des contrôles "soft" par rapport aux contrôles techniques.

Les travaux de Demirović et ses collègues (2021) dans "Internal Audit Risk Assessment in the Function of Fraud Detection" complètent cette analyse en démontrant l'efficacité pratique des matrices de risques dans l'identification des zones de vulnérabilité. Leur étude montre comment l'utilisation structurée de ces outils permet aux **auditeurs internes** de prioriser leurs interventions et d'optimiser l'allocation des ressources de contrôle, particulièrement dans des environnements où les ressources sont limitées.

2.4.1.2 Outils technologiques : data analytics, IA et continuous auditing

L'évolution technologique a révolutionné les méthodes de détection de la fraude, offrant des capacités d'analyse qui dépassent largement les possibilités humaines traditionnelles. Les outils de data analytics permettent l'examen de populations complètes plutôt que d'échantillons, tandis que l'intelligence artificielle ouvre la voie à une détection prédictive des anomalies.

Cependant, la recherche révèle une adoption inégale de ces technologies. L'étude de Mangala et Kumari (2017) montre que, malgré leur potentiel théorique, les outils technologiques avancés ne sont pas perçus comme les plus efficaces par les praticiens. Cette divergence entre potentiel technique et perception professionnelle suggère l'existence d'obstacles à l'adoption ou de limitations pratiques non négligeables.

Les travaux de Wahidahwati et Asyik (2022) dans "Determinants of Auditors Ability in Fraud Detection" apportent un éclairage complémentaire en montrant que l'efficacité de ces outils dépend largement des compétences de leurs utilisateurs. Leur recherche identifie l'expérience et la formation comme des déterminants clés de la capacité des **auditeurs internes** à exploiter efficacement les technologies de détection, suggérant que l'investissement technologique doit s'accompagner d'un investissement en formation.

Le continuous auditing, qui permet une surveillance en temps réel des transactions et des processus, représente une évolution majeure dans la philosophie du contrôle. Cette approche transforme la détection de fraude d'une activité périodique vers une surveillance continue, permettant une réaction plus rapide aux anomalies. Toutefois, comme le soulignent Austin (2022) dans "Remembering Fraud in the Future: Investigating and Improving Auditors' Attention to Fraud during Audit Testing", l'efficacité de ces systèmes dépend de la capacité des **auditeurs externes** à maintenir leur attention sur les signaux d'alerte dans un environnement d'information dense.

2.4.1.3 Whistleblowing systems : dispositifs de signalement interne

Les systèmes de signalement interne constituent un maillon essentiel du dispositif de détection, permettant aux employés de rapporter des comportements suspects sans crainte de représailles. Ces dispositifs comblent une lacune importante des contrôles automatisés en s'appuyant sur l'intelligence humaine et la connaissance contextuelle des processus.

La recherche académique confirme l'efficacité de ces systèmes. L'étude de Mangala et Kumari (2017) classe les mécanismes de dénonciation parmi les méthodes les plus efficaces de détection de fraude, particulièrement pour les fraudes internes qui peuvent échapper aux contrôles automatisés. Cette efficacité s'explique par la capacité unique des employés à détecter des anomalies comportementales ou des écarts par rapport aux procédures établies.

Cependant, l'efficacité de ces systèmes dépend largement de la culture organisationnelle. Comme le démontrent Jizi et ses collègues (2017) dans "Fraud: auditors' responsibility or organisational culture", l'existence formelle d'un système de signalement ne garantit pas son utilisation effective. La recherche souligne l'importance du "tone at the top" et de la confiance des employés dans la protection contre les représailles pour assurer le fonctionnement optimal de ces dispositifs.

Les travaux de Petraşcu et Tieanu (2014) dans "The Role of Internal Audit in Fraud Prevention and Detection" ajoutent une dimension importante en montrant comment l'**audit interne** peut jouer un rôle crucial dans la gestion de ces signalements. Leur étude révèle que l'implication de l'audit interne dans le traitement des alertes renforce la crédibilité du système et améliore la qualité des investigations qui en découlent.

2.4.1.4 Intégration et complémentarité des outils

L'analyse de la littérature révèle que l'efficacité optimale n'est pas atteinte par l'utilisation isolée d'un outil particulier, mais par l'intégration intelligente de différentes méthodes complémentaires. Les contrôles traditionnels fournissent une base solide, les technologies apportent une capacité d'analyse étendue, et les systèmes de signalement comblent les lacunes résiduelles.

Cette complémentarité nécessite cependant une coordination entre les différentes fonctions utilisatrices. Comme le suggèrent Wang et Fargher (2017) dans "The effects of tone at the

top and coordination with external auditors on internal auditors' fraud risk assessments", la coordination entre l'**audit interne** et l'**audit externe** améliore l'efficacité globale du dispositif, particulièrement lorsqu'elle s'accompagne d'un partage d'informations sur les outils et les méthodes utilisés.

L'évolution vers des approches intégrées soulève néanmoins des défis organisationnels importants, notamment en termes de gouvernance des données, de coordination des interventions, et de gestion des compétences. Ces défis constituent autant d'opportunités pour optimiser la collaboration entre les différentes fonctions de contrôle.

2.4.2 Bonnes pratiques de collaboration interfonctionnelle

Si la clarté des rôles constitue un prérequis indispensable, elle ne suffit pas à garantir l'efficacité du dispositif anti-fraude. La recherche académique met progressivement en évidence l'importance cruciale des mécanismes de collaboration entre les différentes fonctions de contrôle. Ces mécanismes, lorsqu'ils sont bien conçus et correctement mis en œuvre, créent une synergie qui dépasse la simple addition des contributions individuelles.

2.4.2.1 Partage d'informations et coordination opérationnelle

Le partage d'informations entre l'audit interne, la gestion des risques et l'audit externe constitue le socle de toute collaboration efficace. Cette circulation de l'information permet de créer une vision globale du risque de fraude et d'éviter les angles morts qui pourraient être exploités par des fraudeurs.

Les travaux de Wang et Fargher (2017) démontrent expérimentalement l'efficacité de cette coordination. Leur étude révèle que la collaboration entre l'**audit interne** et l'**audit externe** améliore significativement l'évaluation du risque de fraude, particulièrement dans des environnements où le "tone at the top" présente des faiblesses. Cette coordination agit comme un mécanisme de compensation qui renforce la résilience globale du dispositif de contrôle.

Les réunions tripartites, impliquant les trois fonctions, représentent une pratique émergente particulièrement prometteuse. Ces rencontres permettent un échange direct d'informations, une harmonisation des approches, et une coordination des calendriers d'intervention. Comme le soulignent Al-Dhubaibi et Sharaf-Addin (2022), cette coordination est d'autant plus importante que les **auditeurs internes** et les **auditeurs externes** n'accordent pas la même importance aux différents signaux d'alerte de fraude, créant des risques de divergence d'appréciation.

La recherche de Drogalas et ses collègues (2017) apporte un éclairage complémentaire en montrant que l'efficacité de l'**audit interne** dans la détection de fraude s'améliore lorsque cette fonction bénéficie d'une formation spécialisée et d'un sentiment renforcé de responsabilité. Ces éléments peuvent être développés à travers des programmes de formation conjoints et des échanges réguliers avec les autres fonctions de contrôle.

2.4.2.2 Comités antifraude et gouvernance intégrée

La mise en place de comités antifraude réunissant les trois fonctions constitue une évolution organisationnelle majeure qui institutionnalise la collaboration. Ces structures permettent de dépasser les échanges ponctuels pour créer un cadre permanent de coordination stratégique.

L'efficacité de ces comités dépend largement de leur positionnement dans l'organisation et de leur articulation avec les instances de gouvernance existantes. La recherche de Jizi et ses collègues (2017) souligne l'importance du soutien de la direction générale et du conseil d'administration pour assurer la crédibilité et l'efficacité de ces structures. Sans ce soutien, les comités antifraude risquent de devenir des instances purement formelles sans impact réel sur la gestion du risque.

Les travaux de Petraşcu et Tieanu (2014) complètent cette analyse en montrant comment l'**audit interne** peut jouer un rôle de facilitateur dans ces comités, grâce à sa position transversale et à sa connaissance approfondie de l'organisation. Cette fonction de facilitation est particulièrement importante pour assurer une participation équilibrée de toutes les parties prenantes et éviter la domination d'une fonction sur les autres.

L'étude de Verwey et Asare (2021) apporte une perspective psychologique intéressante en montrant que l'efficacité de la détection de fraude par les **auditeurs externes** dépend de l'interaction entre leur scepticisme professionnel et leur idéalisme éthique. Cette découverte suggère que la composition des comités antifraude devrait tenir compte non seulement des compétences techniques, mais aussi des profils psychologiques complémentaires des participants.

2.4.2.3 Alignement stratégique et pilotage par la gouvernance

L'alignement sur les priorités stratégiques fixées par le conseil d'administration et le comité d'audit constitue un facteur critique de succès pour la collaboration interfonctionnelle. Cet alignement assure que les efforts de chaque fonction convergent vers les objectifs organisationnels et évite la dispersion des ressources.

La recherche académique confirme l'importance de cet alignement stratégique. Les travaux de DeZoort et Harrison (2016) montrent que le sentiment de responsabilité des auditeurs face à la fraude est influencé par la clarté des attentes organisationnelles et par le soutien perçu de la hiérarchie. Cette dimension psychologique de la responsabilité affecte directement la qualité de la collaboration entre les différentes fonctions.

L'étude de Demirović et ses collègues (2021) illustre concrètement cette importance de l'alignement en montrant comment l'utilisation d'outils communs, comme les matrices de risques, facilite la coordination entre les fonctions. Ces outils partagés créent un langage commun et permettent une priorisation cohérente des efforts de contrôle.

Les mécanismes de reporting intégré constituent un autre levier d'alignement stratégique. En consolidant les informations provenant des trois fonctions, ces mécanismes permettent aux instances de gouvernance d'avoir une vision globale du risque de fraude et de prendre des décisions éclairées sur l'allocation des ressources.

2.4.3 Enjeux et défis de la collaboration

Après avoir identifié les bonnes pratiques de collaboration, il convient d'analyser les obstacles qui peuvent entraver leur mise en œuvre. La recherche académique révèle que la collaboration interfonctionnelle, bien qu'elle soit théoriquement souhaitable, se heurte à des défis pratiques significatifs qui trouvent leurs racines dans les différences organisationnelles, culturelles et professionnelles entre les fonctions.

2.4.3.1 Risques de duplication et zones grises dans la couverture

L'un des paradoxes de la collaboration réside dans le risque de créer des inefficiences par duplication des efforts, tout en laissant subsister des zones non couvertes par aucune fonction. Cette problématique révèle la complexité de la coordination entre des fonctions aux périmètres parfois flous.

Les travaux d'Al-Dhubaibi et Sharaf-Addin (2022) illustrent concrètement cette difficulté. Leur étude montre que les **auditeurs internes** et les **auditeurs externes** n'accordent pas la même importance aux signaux d'alerte de fraude définis par l'ISA 240. Cette divergence de perception peut conduire soit à une duplication des efforts sur certains risques jugés prioritaires par les deux fonctions, soit à des lacunes sur des risques considérés comme secondaires par chacune d'elles.

La recherche de Simon et ses collègues (2018) apporte un éclairage complémentaire en révélant que les méthodes d'évaluation des risques recommandées par les normes peuvent paradoxalement conduire les **auditeurs externes** à sous-estimer certains risques de fraude. Cette découverte suggère que l'harmonisation des méthodes entre les fonctions ne garantit pas nécessairement une couverture optimale des risques.

Les travaux de Demirović et ses collègues (2021) montrent comment l'utilisation d'outils structurés comme les matrices de risques peut aider à résoudre cette problématique. Leur étude révèle que ces outils permettent aux **auditeurs internes** de mieux coordonner leurs interventions avec les autres fonctions, réduisant ainsi les risques de duplication tout en assurant une couverture complète des zones à risque.

2.4.3.2 Enjeux de confiance et de confidentialité des informations

La collaboration interfonctionnelle implique nécessairement un partage d'informations sensibles, ce qui soulève des questions délicates de confidentialité et de confiance mutuelle. Ces enjeux sont particulièrement aigus dans le contexte de la fraude, où les informations partagées peuvent avoir des conséquences juridiques et réputationnelles importantes.

L'étude de Jizi et ses collègues (2017) souligne l'importance de la confiance dans l'efficacité des dispositifs anti-fraude. Leur recherche montre que la défiance entre les fonctions peut compromettre l'efficacité globale du dispositif, les professionnels hésitant à partager des informations sensibles par crainte qu'elles ne soient mal utilisées ou divulguées.

La position particulière de l'**audit externe** complique cette problématique. Comme le démontrent DeZoort et Harrison (2016), les **auditeurs externes** ont un sentiment de responsabilité différent de celui des **auditeurs internes**, ce qui peut affecter leur disposition à partager certaines informations. Cette différence de perspective peut créer des asymétries d'information qui nuisent à l'efficacité de la collaboration.

Les travaux de Petraşcu et Tieanu (2014) suggèrent que l'**audit interne**, de par sa position interne à l'organisation, peut jouer un rôle de facilitateur dans la gestion de ces enjeux de confidentialité. Leur étude montre comment cette fonction peut servir d'interface entre les différents acteurs, en filtrant et en contextualisant les informations partagées.

La recherche d'Austin (2022) ajoute une dimension cognitive à cette problématique en montrant que les **auditeurs externes** peuvent avoir des difficultés à traiter efficacement un volume important d'informations partagées. Cette limitation cognitive peut réduire l'efficacité du partage d'informations si les mécanismes de collaboration ne sont pas adaptés aux capacités de traitement des utilisateurs.

2.4.3.3 Freins culturels et organisationnels

Les différences de culture professionnelle entre les fonctions constituent peut-être l'obstacle le plus fondamental à une collaboration efficace. Chaque fonction a développé ses propres normes, ses propres méthodes, et sa propre vision de la gestion des risques, créant des barrières culturelles qui peuvent être difficiles à surmonter.

L'étude de Verwey et Asare (2021) révèle que l'efficacité de la détection de fraude par les **auditeurs externes** dépend de traits de personnalité spécifiques (scepticisme et idéalisme éthique). Cette découverte suggère que les différences individuelles peuvent affecter la collaboration, certains profils étant plus enclins à la coopération que d'autres.

Les travaux de Wang et Fargher (2017) montrent que l'efficacité de la coordination entre l'**audit interne** et l'**audit externe** dépend largement du "tone at the top". Cette dépendance révèle que les freins culturels ne se limitent pas aux relations entre les fonctions, mais s'enracinent dans la culture organisationnelle globale.

La recherche de Drogalas et ses collègues (2017) apporte un éclairage sur les leviers d'action possibles. Leur étude montre que la formation et le développement du sentiment de responsabilité des **auditeurs internes** peuvent améliorer leur efficacité. Cette conclusion suggère que les investissements en formation et en développement culturel peuvent contribuer à surmonter les freins organisationnels.

Les travaux de Wahidahwati et Asyik (2022) complètent cette analyse en identifiant l'éthique personnelle comme un déterminant clé de l'efficacité des auditeurs. Cette dimension éthique peut constituer un terrain d'entente entre les différentes fonctions, malgré leurs différences méthodologiques.

2.4.4 Opportunités offertes par les nouvelles technologies

L'évolution technologique transforme radicalement le paysage de la lutte contre la fraude, offrant des opportunités inédites pour améliorer à la fois l'efficacité de la détection et la qualité de la collaboration entre les différentes fonctions de contrôle. Ces innovations ne se contentent pas d'automatiser les processus existants ; elles redéfinissent les possibilités d'action et créent de nouveaux modèles de coopération interfonctionnelle.

2.4.4.1 Data analytics avancés et intelligence artificielle : vers une détection prédictive

Les technologies d'analyse de données avancées et d'intelligence artificielle révolutionnent les capacités de détection de fraude en permettant l'examen de populations complètes plutôt que d'échantillons, et en identifiant des patterns complexes invisibles à l'analyse humaine traditionnelle.

L'automatisation des contrôles représente l'une des applications les plus prometteuses de ces technologies. Contrairement aux contrôles manuels traditionnels, les systèmes automatisés peuvent fonctionner en continu, analysant chaque transaction en temps réel et signalant immédiatement les anomalies. Cette capacité de surveillance permanente transforme la philosophie du contrôle, passant d'une logique de vérification périodique à une logique de surveillance continue.

Cependant, la recherche académique révèle que l'efficacité de ces outils dépend largement des compétences de leurs utilisateurs. Les travaux de Wahidahwati et Asyik (2022) montrent que l'expérience et la formation des **auditeurs internes** constituent des déterminants clés de leur capacité à exploiter efficacement ces technologies. Cette conclusion souligne l'importance de l'investissement en formation pour accompagner l'investissement technologique.

La détection prédictive, rendue possible par l'intelligence artificielle, ouvre des perspectives particulièrement intéressantes. En analysant les patterns historiques et en identifiant les facteurs de risque, ces systèmes peuvent anticiper les tentatives de fraude avant qu'elles ne se concrétisent. Cette capacité prédictive permet de passer d'une logique réactive à une logique préventive, transformant fondamentalement l'approche de la gestion du risque de fraude.

L'étude d'Austin (2022) apporte néanmoins une nuance importante en montrant que les **auditeurs externes** peuvent avoir des difficultés à maintenir leur attention sur les signaux de fraude dans un environnement d'information dense. Cette limitation cognitive suggère que l'efficacité des technologies avancées dépend de leur capacité à présenter l'information de manière adaptée aux capacités de traitement humaines.

2.4.4.2 Blockchain : sécurisation et traçabilité des transactions

La technologie blockchain offre des possibilités révolutionnaires en matière de sécurisation des transactions et de traçabilité des opérations. Son principe de registre distribué et immuable crée un environnement où la falsification des données devient extrêmement difficile, voire impossible.

L'application de la blockchain à la lutte contre la fraude se décline en plusieurs dimensions. La sécurisation des transactions constitue l'application la plus évidente : chaque transaction enregistrée sur la blockchain est cryptographiquement sécurisée et ne peut être modifiée sans laisser de traces. Cette caractéristique rend la manipulation comptable beaucoup plus difficile et facilite la détection des tentatives de falsification.

La traçabilité complète des opérations représente un autre avantage majeur. La blockchain permet de suivre chaque transaction depuis son origine jusqu'à sa finalisation, créant une piste d'audit inaltérable. Cette traçabilité facilite les investigations en cas de suspicion de fraude et permet une reconstitution précise des événements.

Les smart contracts, programmes autonomes exécutés sur la blockchain, offrent des possibilités d'automatisation des contrôles particulièrement intéressantes. Ces contrats peuvent intégrer des règles de contrôle qui s'exécutent automatiquement lors de chaque transaction, créant un système de contrôle permanent et incontournable.

2.4.4.3 Facilitation de la coopération interservices

Au-delà de leurs applications directes à la détection de fraude, les nouvelles technologies créent des opportunités inédites pour améliorer la collaboration entre les différentes fonctions de contrôle.

Les plateformes collaboratives permettent un partage d'informations en temps réel entre l'audit interne, la gestion des risques et l'audit externe. Ces outils dépassent les limitations des échanges traditionnels (emails, réunions) en créant des espaces de travail partagés où les informations sont centralisées et accessibles à tous les acteurs autorisés.

La recherche de Wang et Fargher (2017) démontre l'importance de cette coordination en montrant que la collaboration entre l'**audit interne** et l'**audit externe** améliore l'évaluation du risque de fraude. Les technologies collaboratives peuvent faciliter cette coordination en automatisant les échanges d'informations et en créant des référentiels partagés.

Les systèmes de gestion des connaissances permettent de capitaliser sur l'expérience collective des différentes fonctions. En centralisant les retours d'expérience, les bonnes pratiques, et les leçons apprises, ces systèmes créent une mémoire organisationnelle qui bénéficie à toutes les fonctions.

L'intelligence artificielle peut également faciliter la coordination en analysant les patterns de collaboration et en suggérant des améliorations. Ces systèmes peuvent identifier les

redondances, les lacunes de couverture, et les opportunités d'optimisation de la répartition des tâches entre les fonctions.

2.5 Conclusion

Au terme de cette revue de littérature, notre analyse révèle un paysage théorique riche qui éclaire les potentialités et les limites de la collaboration dans la lutte contre la fraude. Le triangle de la fraude de Cressey demeure un modèle explicatif central, enrichi par la recherche contemporaine qui intègre les dimensions psychologiques, organisationnelles et technologiques.

L'analyse des rôles révèle une architecture théorique cohérente où chaque fonction occupe une position complémentaire. L'audit interne constitue le pilier central du dispositif, la gestion des risques apporte une vision stratégique transversale, et l'audit externe renforce la crédibilité par son indépendance. Les cadres normatifs, particulièrement le Three Lines Model et l'ISA 240, érigent cette complémentarité en obligation professionnelle.

Cependant, notre analyse révèle des tensions entre aspirations théoriques et réalités pratiques. La recherche empirique met en évidence des divergences de perception, des biais cognitifs et des différences culturelles qui compliquent la coordination. Cette tension entre prescription normative et réalité comportementale constitue l'un des défis majeurs identifiés.

Notre analyse met également en évidence une lacune significative dans la littérature académique. Si de nombreuses études ont exploré l'efficacité de chaque fonction isolément, peu de travaux se sont penchés sur les dynamiques tripartites concrètes. De plus, la plupart des études adoptent une approche quantitative qui ne capture pas la richesse des mécanismes organisationnels et humains sous-tendant la collaboration.

Cette revue de littérature a établi le socle théorique nécessaire à notre investigation empirique. Elle a identifié les concepts clés, délimité les enjeux, et révélé les zones d'ombre qui méritent un approfondissement, justifiant le choix d'une méthodologie qualitative capable de saisir la complexité des interactions dans la lutte contre la fraude.

3 Chapitre III : Méthodologie de recherche

3.1 Introduction

Après avoir établi le cadre conceptuel et normatif de notre sujet à travers la revue de la littérature, il convient désormais de passer à l'étude empirique. Cette troisième partie du mémoire a pour objectif de décrire la méthodologie mise en œuvre pour répondre à la question centrale de notre recherche : **Comment l'audit interne, la gestion des risques et l'audit externe peuvent-ils collaborer efficacement pour lutter contre la fraude au sein des entreprises ?**

En raison de la complexité du sujet, qui entremêle des normes professionnelles, des cultures d'entreprise, des dynamiques interpersonnelles et des jugements subjectifs, une méthodologie qualitative a été privilégiée. L'objectif de cette recherche est d'examiner en profondeur les perceptions, les expériences et les pratiques de collaboration des professionnels sur le terrain : auditeurs internes, gestionnaires de risques et auditeurs externes.

Ce chapitre détaillera ainsi :

La justification de la méthodologie choisie, qui repose sur une approche qualitative à travers des entretiens semi-directifs.

Le processus de sélection des participants.

La conception du guide d'entretien.

La méthodologie de collecte et d'analyse des données.

La rigueur de la méthode choisie vise à garantir la validité et la pertinence des résultats obtenus, afin d'enrichir la réflexion théorique par des données concrètes issues de l'expérience pratique des acteurs clés de la lutte contre la fraude.

3.2 Justification du choix de la méthode utilisée

Le choix d'une méthodologie de recherche doit être en parfaite adéquation avec la nature de la problématique étudiée. Notre mémoire ne cherche pas à mesurer la fréquence d'un phénomène, mais à **comprendre les dynamiques complexes et souvent subtiles de la collaboration** entre l'audit interne, la gestion des risques et l'audit externe dans la lutte contre la fraude. Il s'agit d'explorer le "comment" et le "pourquoi" de leurs interactions : comment partagent-ils l'information ? Pourquoi la confiance s'installe-t-elle ou, au contraire, se dégrade-t-elle ? Quels sont les arbitrages, les non-dits et les routines qui façonnent leur coopération au quotidien ?

Cette problématique, centrée sur les processus humains et organisationnels, rend une approche purement quantitative inadéquate. Une telle approche pourrait mesurer la fréquence des réunions, mais elle ne pourrait pas saisir la qualité des échanges qui s'y

tiennent. Elle pourrait quantifier le nombre de rapports partagés, mais pas la confiance avec laquelle ils sont reçus et utilisés. Les dimensions que nous cherchons à explorer la culture, la perception, le jugement professionnel, les jeux d'acteurs sont difficilement réductibles à des variables chiffrées.

Pour ces raisons, nous avons résolument opté pour une **méthodologie qualitative**, dont l'outil principal sera l'**entretien semi-directif** mené auprès des professionnels des trois fonctions. Ce choix stratégique est motivé par plusieurs justifications fondamentales :

Explorer un "angle mort" de la recherche : Comme notre revue de littérature l'a montré, si le rôle de chaque fonction est bien documenté, l'étude empirique de leur *interaction* dans le contexte de la fraude reste un domaine peu exploré. L'approche qualitative est par nature exploratoire et donc parfaitement adaptée pour défricher un sujet où les dynamiques réelles sont encore mal comprises.

Saisir la richesse des pratiques de terrain : La lutte contre la fraude n'est pas qu'une affaire de procédures. Elle est faite de jugements, d'intuitions et d'adaptations constantes. Les entretiens semi-directifs offrent la flexibilité nécessaire pour capturer cette richesse. Ils permettent non seulement de couvrir les thèmes prédéfinis, mais aussi de laisser les professionnels illustrer leurs propos par des exemples concrets, des anecdotes et des retours d'expérience qui sont une source de données d'une profondeur inégalée.

Comprendre les perceptions et les représentations : Notre revue de littérature a mis en évidence que les auditeurs internes et externes n'ont pas toujours la même perception du risque ou de leurs responsabilités. L'approche qualitative est la seule à même de creuser ces différences de représentations. Elle permet de "reconstituer le sens donné par les acteurs à leurs pratiques" , ce qui est précisément notre objectif : comprendre comment un auditeur interne, un gestionnaire de risques et un auditeur externe perçoivent leur rôle respectif et celui des autres, et comment ces perceptions influencent leur manière de collaborer.

Identifier les freins implicites : Les obstacles à la collaboration ne sont pas toujours formels ou avoués. Ils peuvent être liés à des questions de culture d'entreprise, de protection de territoire ou de simples habitudes de travail. Seul un dialogue ouvert, tel que le permet l'entretien qualitatif, peut faire émerger ces freins implicites et aider à comprendre pourquoi des collaborations, pourtant logiques sur le papier, échouent dans la pratique.

En conclusion, l'approche qualitative n'est pas un choix par défaut, mais une décision méthodologique délibérée, dictée par la nature même de notre objet de recherche. Elle est la plus à même de fournir une compréhension fine et contextuelle des dynamiques de collaboration, de confronter les exigences normatives aux réalités du terrain, et de générer des enseignements riches pour les professionnels comme pour la recherche académique.

3.3 Processus de sélection des participants

La qualité et la crédibilité d'une recherche qualitative reposent de manière critique sur le choix des participants. La pertinence, l'expérience et la diversité des profils interrogés conditionnent directement la richesse et la validité des données collectées. L'objectif de notre étude étant de comprendre les dynamiques de collaboration entre l'audit interne, la gestion des risques et l'audit externe, il est impératif de recueillir le point de vue de chacune de ces trois fonctions pour obtenir une vision à 360 degrés du phénomène.

La stratégie de sélection des participants a donc été guidée par deux principes fondamentaux :

1. **La pertinence de l'expérience :** Interroger des professionnels ayant une expérience concrète et significative de la gestion du risque de fraude et des interactions inter-fonctions.
2. **La diversification des profils :** Rechercher une variété de points de vue en interrogeant des professionnels issus de contextes organisationnels, géographiques et hiérarchiques différents, conformément aux bonnes pratiques de la recherche qualitative.

Pour répondre à notre problématique, trois catégories de professionnels ont été ciblées, représentant les trois piliers de notre étude.

Catégorie 1 : Les professionnels de l'Audit Interne

Cette catégorie constitue le premier pilier de notre échantillon. les auditeurs internes sont au cœur des processus de contrôle et ont une obligation normative de coordonner leurs travaux avec les autres fonctions d'assurance. Leur perception de la collaboration est donc essentielle. Les profils recherchés incluront :

- **Responsables de l'audit interne (ou Head of Internal Audit)**
- **Managers ou Superviseurs en audit interne**

Leur sélection se basera sur leur expérience dans la planification et la réalisation de missions liées à la fraude, leur implication dans la gouvernance des risques et leur expérience des interactions avec les auditeurs externes et les gestionnaires de risques.

Catégorie 2 : Les professionnels de la Gestion des Risques

Incarnant la "deuxième ligne de défense", les gestionnaires de risques sont responsables de la conception du cadre de gestion du risque de fraude. Leur vision est complémentaire à celle des auditeurs, car ils sont davantage impliqués dans la conception et l'animation du dispositif que dans son évaluation indépendante. Les profils ciblés seront :

- **Responsables de la gestion des risques (ou Chief Risk Officer)**
- **Risk Managers**

Leur expérience dans l'élaboration de cartographies des risques de fraude, la définition de plans d'atténuation et leur rôle d'interface avec le comité d'audit et les autres fonctions de contrôle seront des critères de sélection clés.

Catégorie 3 : Les professionnels de l'Audit Externe

Cette catégorie est indispensable pour comprendre la perspective de l'acteur externe, dont le mandat et les contraintes sont différents. Leur témoignage est crucial pour analyser les frictions et les synergies "vues de l'extérieur". Les profils interrogés seront des professionnels expérimentés, ayant une connaissance approfondie de la norme ISA 240 :

- **Réviseurs d'entreprises / Commissaires aux comptes**
- **Managers et Senior Managers en audit externe**

Afin d'assurer une richesse et une transférabilité des résultats, une diversification sera recherchée au sein de ces trois catégories, notamment sur les dimensions suivantes :

- **Géographique :** Les participants proviendront de plusieurs pays (Belgique, Luxembourg ,France, Maroc) afin de tenir compte des éventuelles spécificités culturelles ou réglementaires locales.
- **Organisationnelle :** Les professionnels pourront être issus de grands cabinets internationaux (Big Four), de cabinets de taille moyenne, ou travailler au sein d'entreprises de secteurs variés (Banque,Assurances,industrie, services, secteur financier).

Le nombre d'entretiens visé se situe **entre 8 et 10**, répartis de manière équilibrée entre les trois catégories de professionnels. Cette taille d'échantillon est jugée suffisante pour une recherche qualitative de ce type, l'objectif étant d'atteindre un point de saturation thématique le stade où les nouveaux entretiens n'apportent plus d'informations substantiellement nouvelles, plutôt qu'une représentativité statistique.

3.4 Outil de collecte des données : le guide d'entretien semi-directif

Dans le cadre de cette étude qualitative, l'outil principal de collecte des données empiriques est un **guide d'entretien semi-directif**. Cette approche a été choisie pour sa capacité à allier structure et flexibilité. D'une part, elle garantit que tous les thèmes essentiels à la problématique de recherche sont abordés avec chaque participant, assurant ainsi la comparabilité des données. D'autre part, elle offre la souplesse nécessaire pour laisser les professionnels développer leurs propres idées, illustrer leurs propos par des exemples concrets et aborder des aspects non anticipés, ce qui est crucial pour une analyse en profondeur.

L'objectif de ce guide est d'explorer les pratiques réelles de collaboration entre l'audit interne, la gestion des risques et l'audit externe, en les confrontant aux cadres normatifs (Normes IIA, ISA 240) et théoriques (Modèle des Trois Lignes, COSO ERM) présentés dans notre revue de littérature. Il s'agit de comprendre comment la coopération se matérialise sur le terrain, quels en sont les facilitateurs, les freins, et comment les professionnels perçoivent leur propre rôle et celui des autres dans le dispositif global de lutte contre la fraude.

Conception et structure du guide d'entretien

Le guide d'entretien a été structuré en sept axes thématiques progressifs, conçus pour explorer de manière systématique les différentes dimensions de la collaboration dans la lutte contre la fraude. Cette architecture permet d'aborder la problématique selon une logique qui va du général au particulier, en partant du contexte professionnel pour aboutir aux recommandations prospectives.

Axe 1 : Informations générales et contexte professionnel Cet axe introductif vise à établir le profil du participant et à contextualiser ses réponses ultérieures. Il explore le poste actuel, l'expérience professionnelle dans le domaine du contrôle, et l'exposition concrète de l'organisation aux cas de fraude. Cette mise en contexte permet de mieux interpréter les perceptions et les pratiques décrites par la suite.

Axe 2 : Perception des rôles et responsabilités Cette section sonde la représentation que le professionnel se fait de l'architecture de contrôle et de sa propre mission. L'objectif est d'identifier les éventuels décalages entre les modèles théoriques et la perception pratique des responsabilités, ainsi que de déceler d'éventuelles confusions ou chevauchements entre les fonctions. Cette exploration permet de comprendre comment chaque acteur positionne sa contribution par rapport à celle des autres.

Axe 3 : Références normatives et professionnalisme Cet axe examine la connaissance et l'application des cadres normatifs, particulièrement l'ISA 240 et les normes IIA. Il explore comment ces références influencent la pratique quotidienne et la collaboration entre fonctions. Cette dimension normative est cruciale pour comprendre les obligations professionnelles qui encadrent la coopération et les éventuelles divergences d'interprétation.

Axe 4 : Collaboration et coordination entre fonctions Au cœur de notre problématique, cet axe investigue les modalités concrètes de la collaboration. Il explore la fréquence des interactions, l'existence de dispositifs formels de coordination, la qualité perçue de la collaboration actuelle, ainsi que les freins et les leviers identifiés par les praticiens. Cette section permet de saisir la réalité opérationnelle de la coopération tripartite.

Axe 5 : Méthodologies, outils et partage d'information Cette section examine les aspects techniques et opérationnels de la collaboration. Elle explore les outils utilisés, les modalités de partage d'information, l'existence de processus formalisés, et les risques de redondance ou de duplication. L'objectif est de comprendre comment les aspects techniques facilitent ou entravent la coordination entre les fonctions.

Axe 6 : Rôle de l'intelligence artificielle et technologies Cet axe prospectif examine l'impact des nouvelles technologies sur la collaboration. Il explore l'utilisation actuelle des outils de data analytics et d'intelligence artificielle, leur potentiel d'amélioration de la coopération, ainsi que les limites et défis de leur adoption. Cette dimension technologique permet d'anticiper les évolutions futures de la collaboration.

Axe 7 : Bonnes pratiques et recommandations L'axe conclusif sollicite une réflexion prospective de la part du professionnel. Il vise à recueillir des exemples de bonnes pratiques, des recommandations d'amélioration, et une réflexion sur le rôle de la culture organisationnelle. Cette section permet de capitaliser sur l'expérience des praticiens pour formuler des recommandations concrètes.

Ce guide a été conçu pour favoriser un échange ouvert et approfondi, avec des questions suffisamment larges pour permettre aux participants d'exprimer leurs expériences personnelles tout en couvrant systématiquement les dimensions clés de notre problématique. La formulation des questions privilégie l'exploration des perceptions, des pratiques vécues, et des recommandations issues de l'expérience terrain, conformément à notre approche qualitative. Il sera clairement précisé

à chaque professionnel que ses propos seront traités de manière anonyme et confidentielle, conformément aux principes d'éthique de la recherche.

3.5 Méthode d'analyse des données

Une fois les entretiens réalisés, une phase cruciale consiste à analyser les données collectées pour en extraire des conclusions significatives et répondre à la problématique de recherche. Compte tenu de la nature qualitative de notre étude, l'approche retenue est une **analyse thématique**. Cette méthode vise à identifier, analyser et interpréter les thèmes, les idées et les schémas récurrents qui émergent des discours des participants. Elle est particulièrement adaptée pour synthétiser les points de vue issus de différents entretiens et pour construire une compréhension globale des dynamiques de collaboration.

Le processus d'analyse se déroulera en plusieurs étapes structurées pour garantir la rigueur et la traçabilité des résultats.

1. Transcription et préparation des données : La première étape consistera à retranscrire intégralement chaque entretien. Cette transcription textuelle est indispensable pour permettre une analyse fine et précise du contenu. Afin de garantir une confidentialité absolue, chaque transcription sera anonymisée : les noms des participants, des entreprises ou toute autre information identifiable seront remplacés par des codes (par exemple, "PA1", "PB 2", "PB 3"). Cette étape assure le respect des engagements pris auprès des participants.

2. Analyse transversale et interprétation : Une fois l'ensemble des entretiens codé, une analyse transversale sera menée. Elle consistera à regrouper les extraits associés à un même thème pour comparer les discours des participants. Cette comparaison s'effectuera selon plusieurs axes :

- **Par fonction :** Quelles sont les convergences et les divergences de points de vue entre les auditeurs internes, les gestionnaires de risques et les auditeurs externes sur un même sujet (par exemple, l'utilité des réunions tripartites) ?
- **Par contexte :** Des différences de pratiques apparaissent-elles en fonction du pays ou de la taille de l'organisation ?
- **Par thématique :** Quels sont les freins les plus fréquemment cités ? Quelles sont les bonnes pratiques qui semblent faire consensus ?

L'objectif de cette étape est de dépasser la simple description des discours pour les interpréter, c'est-à-dire identifier des tendances, expliquer les divergences et confronter les pratiques de terrain aux cadres théoriques et normatifs établis dans la revue de littérature.

3. Limites de la méthode d'analyse : Comme toute approche qualitative, cette méthode comporte des limites qu'il convient de reconnaître. La **taille limitée de l'échantillon**, bien qu'appropriée pour une analyse en profondeur, ne permet pas de généraliser statistiquement les résultats à l'ensemble des professionnels. De plus, l'interprétation des données comporte une part de **subjectivité** de la part du chercheur. Pour atténuer ce biais, la démarche d'analyse sera la plus transparente possible, en s'appuyant sur des citations directes des participants pour illustrer chaque conclusion. Enfin, un **biais de désirabilité sociale** peut amener certains participants à présenter une version idéalisée de leurs pratiques. La triangulation des points de vue entre les trois fonctions visera à limiter cet effet.

Malgré ces limites, la rigueur du processus d'analyse thématique et la richesse des données collectées permettront de produire une analyse nuancée et argumentée, capable de répondre de manière approfondie à notre problématique de recherche.

4 Chapitre IV : Résultats de l'étude empirique

4.1 Introduction :

Les chapitres précédents ont établi le cadre théorique de notre recherche en explorant les fondements de la fraude, les responsabilités de l'audit interne, de la gestion des risques et de l'audit externe selon les référentiels professionnels (normes IIA, ISA 240, COSO ERM), ainsi que les enjeux de leur collaboration.

Toutefois, la théorie ne suffit pas à saisir la complexité du terrain. Les normes définissent des périmètres, mais elles ne disent pas toujours comment ces périmètres s'articulent concrètement dans le quotidien des organisations. C'est pour combler cet écart que nous avons mené une enquête empirique auprès de neuf professionnels : auditeurs externes, auditeurs internes et responsables de la gestion des risques.

Cette quatrième partie présente les résultats de l'analyse qualitative menée à partir des entretiens semi-directifs. L'objectif est triple : synthétiser les observations sur les perceptions et pratiques actuelles, identifier les défis qui entravent la collaboration, et mettre en évidence les bonnes pratiques suggérées par les répondants.

4.2 Synthèse des observations : Perceptions, pratiques et réalités du terrain

4.2.1.1 La perception des rôles et responsabilités

L'un des constats les plus marquants de notre enquête empirique concerne l'écart parfois entre la clarté théorique des rôles, telle que définie par les référentiels professionnels, et la confusion qui persiste dans la pratique quotidienne des organisations. Cette tension apparaît de manière récurrente dans les témoignages recueillis, révélant une réalité plus nuancée que ne le laissent supposer les normes.

4.2.1.2 L'audit externe : entre scepticisme professionnel et limites du mandat

Les professionnels de l'audit externe interrogés manifestent une compréhension claire de leur mission telle que définie par la norme ISA 240. Leur discours converge autour de deux piliers fondamentaux : le maintien d'un **scepticisme professionnel** constant et la reconnaissance explicite des limites de leur responsabilité en matière de fraude. Cette position est résumée de manière frappante par l'un des senior managers interrogés : *"on n'est pas des détectives, on fait de l'audit"*. Cette formule, reprise sous différentes formes par plusieurs répondants, illustre la volonté de délimiter clairement le périmètre d'intervention de l'audit externe.

Un réviseur d'entreprises agréé développe cette idée en précisant que l'auditeur externe n'est pas là pour "anticiper, détecter ou corriger les cas de fraude", mais uniquement pour s'assurer que l'opinion émise sur les états financiers atteste d'une image sincère exempte d'anomalies significatives provenant de fraudes ou d'erreurs. Cette distinction, conforme à

l'esprit de l'ISA 240, souligne que la mission première reste l'audit des comptes et non l'investigation de fraude.

Au-delà de cette clarté conceptuelle, les entretiens révèlent également une conscience aiguë des obligations de reporting qui pèsent sur les auditeurs externes, particulièrement dans le contexte luxembourgeois. Ces obligations incluent le signalement à la Cellule de Renseignement Financier (CRF) pour les infractions de premier degré incluant la fraude, la notification à la CSSF en cas de démission pour juste motif lié à l'intégrité de la direction, et la communication au Commissariat aux assurances pour le secteur spécifique des assurances.

4.2.1.3 L'audit interne : un positionnement stratégique théorique confronté à des réalités variables

Si les normes IIA positionnent l'audit interne comme une fonction stratégique dotée d'une mission d'assurance et de conseil, la réalité du terrain révèle une situation plus hétérogène. Théoriquement, l'audit interne devrait jouer un rôle stratégique, mais dans la pratique, cela dépend de l'organisation. Certains audits internes disposent d'une véritable indépendance, tandis que d'autres sont limités par leur positionnement hiérarchique ou leurs ressources.

Cette variabilité s'explique par deux facteurs principaux. D'abord, le rattachement hiérarchique : l'efficacité de la fonction dépend fondamentalement de son indépendance et de son intégration dans la gouvernance. Ensuite, les ressources allouées : plusieurs répondants évoquent la rareté des services d'audit interne véritablement opérationnels, particulièrement dans les structures de taille moyenne. Cette absence transforme le travail de l'audit externe, qui doit alors réaliser davantage de travaux substantifs.

4.2.1.4 La gestion des risques : une fonction de liaison.

Certains répondants attribuent à la gestion des risques un rôle essentiellement préventif, la distinguant de l'audit interne. Toutefois, d'autres notent que cette fonction dispose dans ses attributions la lutte contre la fraude de manière explicite. Elle est généralement responsable d'une variété de risques (financier, opérationnel, humain, légal, environnemental) mais .

Le témoignage d'une directrice de pôle Contrôle Permanent et Risques Opérationnels dans le secteur bancaire offre un contraste saisissant. Elle décrit sa fonction comme le cœur du métier en matière de lutte contre la fraude, avec une mission claire de prévenir et piloter la réponse opérationnelle. Cette vision illustre la diversité des modèles organisationnels et suggère que le positionnement de la gestion des risques dépend fortement du secteur d'activité et de la maturité de l'organisation.

4.2.2 L'état de la collaboration : entre nécessité reconnue et mise en œuvre limitée

Au-delà de la clarté des rôles individuels, la question centrale porte sur la manière dont ces trois fonctions collaborent effectivement dans la lutte contre la fraude.

4.2.2.1 Une fréquence de coordination très variable

L'analyse des témoignages révèle une disparité considérable dans la fréquence des interactions entre les trois fonctions. De nombreux professionnels de l'audit externe déclarent travailler très rarement en coordination avec les autres fonctions, reflétant une réalité où les fonctions d'audit interne ou de gestion des risques sont souvent absentes ou sous-développées dans les structures de taille moyenne.

À l'inverse, les professionnels du secteur financier décrivent une coordination intensive et multi-niveaux : journalière ou hebdomadaire avec la Conformité, mensuelle en comité fraude, et trimestrielle en comités de gouvernance.

4.2.2.2 Des dispositifs formels rares et concentrés dans les grandes structures

L'existence de dispositifs formels de coordination constitue un indicateur clé de la maturité organisationnelle. Les réponses révèlent une concentration de ces dispositifs dans les grandes structures, particulièrement dans le secteur financier fortement régulé. La majorité des répondants issus de l'audit externe ou travaillant avec des PME déclarent ne pas connaître de dispositifs formels de coordination, souvent justifiant cette absence par la taille de la société.

4.2.2.3 Des cas de fraude révélateurs

Les cas concrets de fraude mentionnés illustrent l'importance d'une collaboration effective. Le cas le plus détaillé concerne un directeur général qui utilisait des fonds de la société pour financer son club de football personnel. La détection a été initiée par une alerte du directeur financier qui a contacté directement les auditeurs externes. Ce premier élément souligne l'importance des signaux d'alerte internes et de la capacité des collaborateurs à communiquer leurs préoccupations.

L'investigation a illustré magistralement l'importance de l'observation directe. En se rendant sur place, les auditeurs ont constaté une tension très palpable entre le directeur financier et le directeur général, visible immédiatement dans les échanges et dans la disposition des bureaux.

Ce cas illustre plusieurs points cruciaux. Premièrement, la fraude a été détectée grâce à un signalement interne, soulignant l'importance d'une culture organisationnelle où les employés se sentent en confiance pour alerter. Deuxièmement, l'investigation a nécessité une présence physique sur site, impossible à remplacer par des analyses de données à distance. Troisièmement, la détection a impliqué une collaboration de fait entre plusieurs acteurs.

D'autres cas mentionnés incluent des détournements via carte bancaire, une pyramide de Ponzi détectée grâce au scepticisme professionnel et à des recherches en ligne, ainsi que des fraudes dans la gestion des stocks. Ces cas confirment que la détection de fraude repose souvent sur une combinaison de vigilance humaine, d'observation directe et de collaboration entre les différentes fonctions de contrôle.

4.2.3 L'utilisation des technologies : un potentiel reconnu mais une adoption timide

La question de l'utilisation des technologies, et particulièrement de l'intelligence artificielle et du data analytics, révèle un décalage important entre le potentiel reconnu par tous les répondants et la réalité d'une adoption encore très limitée.

4.2.3.1 Un état des lieux contrasté de l'adoption technologique

La majorité des répondants issus de l'audit externe ou de structures de taille moyenne déclarent ne pas utiliser actuellement d'outils avancés de data analytics ou d'intelligence artificielle. Plusieurs précisent qu'ils vont commencer à se pencher sur la question, mais que pour le moment, ce n'est pas encore le cas. Certains indiquent que leur organisation commence à utiliser des outils d'analyse de données, mais que c'est encore limité par les coûts et la complexité de mise en œuvre. Pour les petites missions, ce n'est pas toujours rentable.

Des professionnels décrivent une situation intermédiaire où l'IA n'est pas encore utilisée, mais des analyses de données sont effectuées via Excel ou Power BI et des outils internes pour détecter les anomalies. Cette approche représente probablement la réalité de nombreuses organisations qui cherchent à améliorer leurs capacités analytiques sans investir massivement dans des technologies de pointe.

À l'autre extrémité du spectre, le secteur bancaire décrit une adoption plus avancée avec l'utilisation de règles de détection et de KRIs (Key Risk Indicators), tandis que l'IA est en phase pilote pour l'analyse de signaux faibles. Le déploiement complet dépend cependant de la qualité des données et de la gouvernance des modèles. Cette formulation révèle que même dans les secteurs les plus avancés, l'IA reste souvent au stade expérimental.

4.2.3.2 Le potentiel des technologies : entre opportunités reconnues et limites dans la coordination

Malgré une adoption encore limitée sur le terrain, l'ensemble des professionnels interrogés reconnaissent le potentiel considérable de l'intelligence artificielle et du data analytics pour améliorer la détection de fraude. Ces technologies permettraient de combler certaines lacunes humaines en offrant une vision plus objective, en facilitant les contrôles, en analysant des volumes de données impossibles à traiter manuellement, et en identifiant des patterns qui échapperaient à l'œil humain. Plusieurs répondants soulignent également leur dimension collaborative potentielle : l'IA pourrait centraliser les signaux faibles, automatiser la détection d'anomalies, prioriser les cas à investiguer, et même identifier les zones non couvertes par les différentes fonctions de contrôle, favorisant ainsi un langage commun entre elles. Toutefois, les avis se nuancent lorsqu'il s'agit d'évaluer l'impact direct de ces technologies sur la collaboration interfonctionnelle. Plusieurs professionnels apportent une distinction importante : si l'intelligence artificielle peut améliorer significativement l'efficacité technique de chaque fonction prise séparément, elle ne remplace pas la communication et la compréhension mutuelle entre les acteurs. La collaboration, selon ces répondants, doit avant tout être améliorée par les humains eux-mêmes, à travers des

changements organisationnels et culturels. La technologie joue ainsi un rôle de support précieux, mais ne peut se substituer aux transformations fondamentales nécessaires pour une coordination véritablement intégrée.

4.2.3.3 Des freins multiples à l'adoption

L'analyse des obstacles révèle une convergence remarquable autour de trois freins principaux : le coût, la formation et la qualité des données. Le coût est mentionné par la quasi-totalité des répondants comme un obstacle majeur. L'investissement technologique doit être proportionné à la taille et à la complexité des missions. Les professionnels travaillant en sous-traitance ajoutent que leurs outils sont utilisés pour de nombreuses sociétés qui disposent de petits budgets et ne sont pas intéressées par des outils coûteux.

La formation constitue le deuxième frein majeur. Il faut former les équipes, ce qui représente un coût et du temps. Le manque de formation du personnel est cité parmi les principales limites. Cette dimension humaine est souvent sous-estimée, disposer d'outils performants ne suffit pas si les utilisateurs ne maîtrisent pas les compétences nécessaires pour les exploiter efficacement.

La qualité des données apparaît comme le troisième obstacle. Il faut que le client ait des données de qualité et soit prêt à investir dans ces technologies. Le déploiement complet de l'IA dépend de la qualité des données et de la gouvernance des modèles.

4.3 Identification des défis : Les obstacles à une collaboration intégrée

La synthèse des observations présentée dans la section précédente a mis en lumière un paradoxe central : alors que la nécessité de la collaboration est unanimement reconnue par les professionnels interrogés, sa mise en œuvre effective demeure largement insuffisante. Cette section se concentre sur l'identification et l'analyse des obstacles qui entravent une collaboration pleinement intégrée entre l'audit interne, la gestion des risques et l'audit externe dans la lutte contre la fraude.

4.3.1 Le défi structurel : La confusion des rôles et le chevauchement des mandats

Le premier défi majeur concerne la clarté des rôles et responsabilités de chaque fonction. Bien que les référentiels professionnels définissent théoriquement des périmètres distincts, la réalité révèle des zones de flou, particulièrement entre l'audit interne et la gestion des risques.

Cette confusion conduit à deux problèmes majeurs. D'une part, une duplication des efforts lorsque plusieurs fonctions réalisent des contrôles similaires, créant un gaspillage de ressources et de la confusion auprès du management. D'autre part, cette situation peut générer des angles morts dans le dispositif de contrôle : lorsque chaque fonction suppose que certains risques sont couverts par une autre, des zones entières échappent à tout contrôle effectif, constituant des failles exploitables par les fraudeurs.

La perception du rôle de l'auditeur externe illustre particulièrement ce défi. Plusieurs répondants soulignent que beaucoup pensent encore que l'auditeur a pour responsabilité de détecter toutes les fraudes. Cette incompréhension peut conduire les autres fonctions à se déresponsabiliser, pensant que l'audit externe détectera nécessairement toute fraude.

4.3.2 Le défi humain et communicationnel : Des silos renforcés par la distance

Au-delà des aspects structurels, les entretiens révèlent un défi majeur lié aux dimensions humaines et communicationnelles de la collaboration, particulièrement illustré par la critique récurrente des échanges virtuels au détriment du contact direct.

Un réviseur d'entreprises agréé le formule clairement : "Il n'y a rien de tel qu'une réunion où tu rencontres les gens ou tu viens te rendre compte des processus sur place. Les outils technologiques de communication ont souvent leurs limites." Cette observation est corroborée par le cas du détournement pour le club de football, où l'observation sur place a permis de détecter la tension palpable entre le directeur financier et le directeur général.

Ce défi est aggravé par l'absence d'instances de coordination formelles dans de nombreuses organisations. Sans cadre structuré, la collaboration reste ponctuelle et réactive. Les freins identifiés incluent le manque de communication continue, l'organisation en silos, la confidentialité de certaines informations, et l'absence de protocoles clairs. Ces obstacles sont particulièrement prononcés dans les modèles de sous-traitance, où la coordination continue devient pratiquement impossible.

4.3.3 Le défi déontologique : La tension entre indépendance et coopération

Un troisième défi majeur, de nature déontologique, concerne la tension inhérente entre l'exigence d'indépendance de l'auditeur externe et la nécessité de collaborer avec les fonctions internes. Cette tension est particulièrement aiguë dans le contexte de la lutte contre la fraude, où le partage d'informations sensibles est crucial mais où l'indépendance de jugement doit être préservée.

Les professionnels de l'audit externe interrogés soulignent qu'ils doivent maintenir un équilibre délicat. D'un côté, ils peuvent et doivent s'appuyer sur les travaux de l'audit interne pour améliorer l'efficacité de leur mission. De l'autre, ils doivent conserver leur indépendance et leur scepticisme professionnel, ne pouvant pas accepter aveuglément les conclusions des fonctions internes. Cette nécessité d'évaluer et de tester les travaux de l'audit interne avant de s'y appuyer peut être perçue comme un manque de confiance et freiner la collaboration.

Les répondants mentionnent la confidentialité, la séparation des tâches et des responsabilités comme principaux freins à une collaboration efficace. Cette préoccupation est légitime : dans certains cas de fraude, le management lui-même peut être impliqué, rendant le partage d'informations avec les fonctions internes potentiellement problématique. Un manager d'audit externe rappelle d'ailleurs qu'en cas de détection de

fraude, il ne faut pas informer le management car celui-ci peut parfois être impliqué dans la fraude.

Cette tension déontologique est particulièrement complexe à gérer dans les organisations de taille moyenne où les relations personnelles sont plus étroites et où la séparation fonctionnelle est moins marquée que dans les grandes structures. Le défi consiste à maintenir la rigueur professionnelle et l'indépendance tout en développant une collaboration suffisamment étroite pour être efficace.

4.4 Bonnes pratiques et leviers d'amélioration

Après avoir identifié les défis qui entravent une collaboration efficace, cette section se veut constructive en mettant en lumière les bonnes pratiques observées et les leviers d'amélioration suggérés par les professionnels eux-mêmes. Ces recommandations, ancrées dans l'expérience concrète des répondants, constituent autant de pistes pour renforcer la collaboration interfonctionnelle dans la lutte contre la fraude.

4.4.1 Le contact humain comme principal levier de synergie

La recommandation la plus unanime et la plus insistante des professionnels interrogés concerne l'importance du contact humain et de la présence physique sur le terrain. Cette recommandation, qui peut sembler évidente ou même anachronique à l'ère de la digitalisation, est pourtant corroborée par l'ensemble des cas de fraude détectés mentionnés par les répondants.

Le cas du détournement pour le club de football illustre parfaitement cette importance. C'est en se rendant sur place que les auditeurs ont pu observer la tension entre le directeur financier et le directeur général, constater la disposition des bureaux, et repérer les éléments visuels (chartes du club, photos) qui ont confirmé l'allégation. Comme le souligne un réviseur d'entreprises : *"Il n'y a rien de tel que d'aller voir sur place et voir si certaines informations peuvent être corroborées par rapport à ce qu'on peut voir, ce qu'on peut entendre."*

Cette importance du contact direct s'explique par plusieurs facteurs. Premièrement, l'observation physique permet de capter des signaux faibles qui ne transparaissent pas dans les documents ou les échanges virtuels : tensions interpersonnelles, incohérences entre le discours et les comportements, éléments visuels révélateurs. Deuxièmement, la présence sur place permet d'évaluer la culture organisationnelle et le "tone at the top" de manière beaucoup plus fine qu'à distance. Troisièmement, les échanges en face-à-face facilitent la construction de la confiance et la qualité de la communication entre les différentes fonctions.

Cette recommandation a des implications importantes pour la collaboration interfonctionnelle. Elle suggère que les réunions de coordination entre audit interne, gestion des risques et audit externe devraient privilégier le format présentiel plutôt que virtuel,

particulièrement lorsqu'il s'agit de discuter de sujets sensibles ou de partager des préoccupations sur des risques de fraude. Elle implique également que les missions d'audit, qu'elles soient internes ou externes, devraient systématiquement inclure une composante d'observation sur site, même lorsque les outils technologiques permettraient théoriquement de réaliser certains contrôles à distance.

4.4.2 La structuration de la communication comme catalyseur

Au-delà du contact humain, les professionnels interrogés soulignent l'importance de structurer la communication entre les trois fonctions à travers des dispositifs formels et des processus clairement définis.

Le premier levier identifié concerne le moment de la communication. Plusieurs répondants insistent sur l'importance d'un dialogue "dès le début de la mission". Cette communication précoce permet de partager les zones de risque identifiées par chaque fonction, de coordonner les calendriers d'intervention pour éviter les redondances, et d'identifier les opportunités de synergie. Un senior manager d'audit externe note que lorsque l'audit interne et la gestion des risques sont bien structurés, on peut échanger sur les zones de risque, partager certaines informations, et éviter de refaire le même travail.

Le deuxième levier concerne la mise en place de réunions de coordination régulières. Les organisations les plus matures en matière de collaboration décrivent des dispositifs multi-niveaux : réunions opérationnelles fréquentes (hebdomadaires ou mensuelles) pour le partage d'information et la coordination des interventions, comités fraude mensuels pour l'examen des alertes et des incidents, et comités de gouvernance trimestriels pour le pilotage stratégique du dispositif anti-fraude. Cette structuration à plusieurs niveaux permet de combiner l'efficacité opérationnelle et la vision stratégique.

Le troisième levier identifié concerne le partage planifié des zones de risque et des plans d'audit. Un réviseur d'entreprises recommande la "communication et coordination anticipative des programmes de testing de l'année". Cette planification concertée permet non seulement d'éviter les redondances, mais aussi de s'assurer qu'aucune zone à risque n'est laissée sans couverture. Elle facilite également l'optimisation des ressources en permettant à chaque fonction de se concentrer sur ses domaines de compétence spécifiques.

Les professionnels du secteur bancaire décrivent des pratiques particulièrement élaborées : plans de contrôle concertés, workflow outillé pour l'escalade des incidents et le suivi des plans d'actions, tableaux de bord trimestriels partagés, et flash reports pour les situations urgentes. Ces outils permettent de formaliser et de systématiser la communication, réduisant ainsi la dépendance aux initiatives individuelles.

4.4.3 L'optimisation de l'existant : S'appuyer sur les travaux des autres fonctions

La troisième catégorie de bonnes pratiques concerne l'utilisation intelligente et critique des travaux réalisés par les autres fonctions. Cette pratique, particulièrement pertinente pour

l'audit externe qui peut s'appuyer sur les travaux de l'audit interne, illustre comment la collaboration peut améliorer l'efficacité globale du dispositif de contrôle.

Les professionnels de l'audit externe soulignent que lorsqu'un audit interne existe et fonctionne bien, ils peuvent s'appuyer sur ses travaux tout en gardant leur indépendance. Cette utilisation des travaux de l'audit interne permet de réduire l'étendue des tests substantifs, d'améliorer la compréhension de l'environnement de contrôle, et de concentrer les efforts sur les zones à plus haut risque. Toutefois, cette utilisation doit s'accompagner d'une évaluation critique de la qualité et de la fiabilité des travaux de l'audit interne.

Cette bonne pratique nécessite plusieurs conditions pour être efficace. Premièrement, l'audit interne doit disposer d'une indépendance suffisante et de compétences adéquates. Deuxièmement, ses travaux doivent être documentés de manière suffisamment détaillée pour permettre leur évaluation par l'audit externe. Troisièmement, il doit exister des canaux de communication permettant à l'audit externe d'accéder aux rapports et aux documents de travail de l'audit interne, dans le respect de la confidentialité.

4.4.4 Les recommandations pour une gouvernance intégrée

Au-delà des pratiques opérationnelles, plusieurs professionnels proposent des recommandations de nature plus stratégique, visant à créer une véritable gouvernance intégrée de la lutte contre la fraude.

La recommandation la plus structurée provient d'un manager d'audit interne qui propose d'"instaurer une gouvernance claire avec une cellule commune antifraude, des réunions périodiques et une charte précisant les rôles et responsabilités de chaque acteur". Cette approche, qui s'apparente au concept d'"integrated assurance" mentionné par un professionnel de l'audit interne, vise à créer une coordination systématique entre les différentes fonctions d'assurance.

Une directrice de gestion des risques recommande d'"avoir un référentiel commun des contrôles et incidents relié à un outillage partagé avec des KRI homogènes et une gouvernance claire des données". Cette recommandation souligne l'importance d'un langage commun et d'outils partagés pour faciliter la collaboration. Lorsque chaque fonction utilise ses propres définitions, ses propres outils et ses propres indicateurs, la coordination devient extrêmement complexe.

Plusieurs répondants insistent sur l'importance du soutien de la direction générale et du conseil d'administration. Sans ce soutien au plus haut niveau, les initiatives de collaboration risquent de rester superficielles et de ne pas disposer des ressources nécessaires. Le "tone at the top" doit clairement promouvoir une culture de conformité, de gestion saine des risques, et de collaboration entre les fonctions de contrôle.

4.5 Conclusion

Cette partie empirique a permis de confronter le cadre théorique établi dans les chapitres précédents aux réalités du terrain, telles qu'elles sont vécues et perçues par les professionnels de l'audit externe, de l'audit interne et de la gestion des risques. L'analyse des entretiens révèle un paysage complexe et contrasté, marqué par un paradoxe central : alors que tous les acteurs reconnaissent l'importance cruciale de la collaboration dans la lutte contre la fraude, sa mise en œuvre effective demeure largement insuffisante.

La synthèse des observations a mis en lumière deux constats majeurs. Premièrement, la collaboration entre les trois fonctions demeure largement ponctuelle et réactive, avec une forte disparité entre les grandes structures du secteur financier, qui disposent de dispositifs formels élaborés, et les organisations de taille moyenne où la coordination est quasi inexistante. Deuxièmement, malgré un potentiel largement reconnu, l'adoption des technologies avancées comme l'intelligence artificielle et le data analytics reste timide, freinée par des obstacles de coût, de formation et de qualité des données.

L'identification des défis a permis de comprendre les raisons profondes de ce paradoxe. Quatre catégories d'obstacles ont été identifiées : des défis structurels liés aux rôles et aux risques de duplication ou d'angles morts ; des défis humains et communicationnels ; des défis déontologiques liés à la tension entre l'exigence d'indépendance et la nécessité de collaborer ; et des défis culturels concernant l'impact de la confiance excessive et la perception négative du contrôle.

Ces constats empiriques posent les bases pour la partie suivante, qui visera à proposer des recommandations concrètes et opérationnelles pour renforcer la collaboration entre l'audit interne, la gestion des risques et l'audit externe dans la lutte contre la fraude. Ces recommandations s'appuieront à la fois sur les bonnes pratiques identifiées dans cette partie et sur les enseignements de la littérature académique et professionnelle analysée dans les chapitres précédents.

5 Chapitre V : Discussion et Recommandations

5.1 Introduction

Les résultats empiriques présentés dans la partie précédente ont révélé un paradoxe central : alors que les référentiels professionnels définissent clairement les rôles et responsabilités de chaque fonction de contrôle, et que tous les acteurs reconnaissent l'importance de la collaboration dans la lutte contre la fraude, la mise en œuvre effective de cette collaboration demeure largement insuffisante. Cette partie vise à confronter ces constats empiriques au cadre théorique établi dans les chapitres précédents, afin de comprendre les raisons profondes de cet écart et de proposer des recommandations concrètes pour le réduire.

Cette discussion s'articulera autour de deux axes complémentaires. Dans un premier temps, nous procéderons à une analyse critique des résultats en les confrontant à la littérature existante et aux référentiels professionnels. Il s'agira de comprendre dans quelle mesure les observations du terrain confirment, nuancent ou contredisent les prescriptions théoriques, et d'identifier les facteurs explicatifs de ces écarts. Dans un second temps, nous formulerons des propositions concrètes visant à renforcer la collaboration entre l'audit interne, la gestion des risques et l'audit externe. Ces recommandations s'appuieront à la fois sur les bonnes pratiques identifiées lors des entretiens et sur les enseignements tirés de la confrontation entre théorie et pratique.

5.2 Analyse critique des résultats : Confrontation entre théorie et pratique

5.2.1 Le modèle des trois lignes de défense :

Le modèle des trois lignes de défense, largement adopté comme cadre de référence pour l'organisation des fonctions de contrôle, repose sur une délimitation claire des responsabilités. La première ligne, constituée du management opérationnel, est propriétaire et gestionnaire des risques au quotidien. La deuxième ligne, comprenant la gestion des risques et la conformité, assure la surveillance, le conseil et le support. La troisième ligne, incarnée par l'audit interne, fournit une assurance indépendante sur l'efficacité des deux premières lignes. L'audit externe, bien qu'externe à ce modèle, interagit avec l'ensemble de ces fonctions pour fournir une assurance indépendante aux parties prenantes externes.

Les résultats empiriques révèlent toutefois une réalité beaucoup plus nuancée. Si les professionnels de l'audit externe manifestent une compréhension claire de leur rôle, conforme aux prescriptions de la norme ISA 240, la situation est plus contrastée pour les fonctions internes. La position de l'audit interne, théoriquement stratégique selon les normes IIA, dépend dans la pratique de facteurs organisationnels variables : rattachement hiérarchique, ressources allouées, et soutien de la direction. Plus problématique encore, la fonction de gestion des risques apparaît comme la moins bien définie, avec un périmètre qui varie considérablement selon les organisations et les secteurs d'activité.

Cette confusion pratique s'explique par plusieurs facteurs que la littérature théorique n'aborde que partiellement. Premièrement, le modèle des trois lignes de défense reste un cadre conceptuel qui nécessite une adaptation au contexte spécifique de chaque organisation. Or, cette adaptation est rarement accompagnée d'une clarification formelle des rôles et responsabilités. Deuxièmement, la distinction entre la gestion des risques (deuxième ligne) et l'audit interne (troisième ligne) peut sembler claire en théorie, mais devient floue dans la pratique, particulièrement en matière d'évaluation des contrôles et d'alerte précoce. Troisièmement, la taille de l'organisation joue un rôle déterminant : dans les structures de taille moyenne, les fonctions de contrôle sont souvent sous-développées, voire absentes, rendant le modèle théorique difficilement applicable.

Cette observation rejoint les travaux de l'Institute of Internal Auditors qui, dans ses standards 2025, reconnaît implicitement cette variabilité en insistant sur la nécessité d'adapter les pratiques au contexte organisationnel. Elle souligne également une limite importante du modèle des trois lignes : sa focalisation sur la structure formelle au détriment des mécanismes de coordination et de collaboration entre les lignes. Le modèle définit ce que chaque ligne doit faire, mais dit peu sur comment elles doivent interagir, laissant cette dimension à la discrétion de chaque organisation.

5.2.2 Le triangle de la fraude et les limites de l'approche par fonction

Le triangle de la fraude de Cressey, qui identifie la pression, l'opportunité et la rationalisation comme les trois éléments constitutifs de tout acte frauduleux, offre un cadre d'analyse particulièrement pertinent pour comprendre les limites d'une approche cloisonnée de la lutte contre la fraude. En effet, chacune des trois fonctions étudiées se concentre naturellement sur l'un des éléments du triangle, sans nécessairement appréhender l'ensemble de manière intégrée.

L'audit interne et la gestion des risques se focalisent principalement sur la réduction des opportunités à travers l'évaluation et le renforcement du contrôle interne. L'audit externe, dans le cadre de sa mission d'audit des états financiers, s'intéresse également aux opportunités, mais sous l'angle spécifique des anomalies significatives dans les comptes. La dimension de la pression, pourtant fondamentale selon le modèle de Cressey, est largement négligée par les trois fonctions, relevant davantage de la responsabilité des ressources humaines ou du management. Quant à la rationalisation, liée à la culture organisationnelle et au "tone at the top", elle est reconnue comme importante par tous les répondants, mais fait rarement l'objet d'une évaluation systématique et coordonnée.

Les cas de fraude mentionnés par les répondants illustrent parfaitement cette limite. Le cas du directeur général détournant des fonds pour son club de football personnel combine les trois éléments du triangle : une pression (besoin de financer le club), une opportunité (contrôles insuffisants sur l'utilisation des fonds), et une rationalisation (probablement liée à sa position de pouvoir). La détection n'est pas venue d'une analyse systématique de ces trois dimensions, mais d'un signalement du directeur financier suivi d'une observation directe sur

place. Ce constat suggère que même lorsque les fonctions de contrôle existent, leur approche fragmentée peut laisser des angles morts.

Cette observation rejoint les travaux récents de l'ACFE (Association of Certified Fraud Examiners) qui soulignent que la détection de fraude repose souvent davantage sur des signalements (tips) que sur les contrôles formels. Dans notre étude, plusieurs répondants confirment cette réalité en insistant sur l'importance d'une culture de transparence et de signalement. Toutefois, la création et le maintien d'une telle culture nécessitent une approche coordonnée impliquant toutes les fonctions de contrôle, ce qui ramène à la question centrale de la collaboration.

5.2.3 La norme ISA 240 et la perception du rôle de l'auditeur externe

La norme ISA 240 définit clairement les responsabilités de l'auditeur externe en matière de fraude : maintenir un scepticisme professionnel, identifier et évaluer les risques de fraude, adapter les procédures d'audit en conséquence, et communiquer de manière appropriée. Elle précise également, de manière tout aussi claire, que l'auditeur n'est pas responsable de la prévention de la fraude et qu'il ne peut garantir la détection de toutes les fraudes, sa mission première restant l'audit des états financiers.

Les entretiens révèlent que cette clarté normative ne se traduit pas par une compréhension uniforme du rôle de l'auditeur externe. Plusieurs répondants soulignent que les clients et les personnes externes au métier pensent souvent à tort que le rôle de l'auditeur est la détection de la fraude. Ce malentendu, loin d'être anodin, a des conséquences importantes. D'une part, il peut créer un faux sentiment de sécurité chez les organisations qui croient que la présence d'un audit externe garantit la détection de toute fraude. D'autre part, il peut conduire les autres fonctions de contrôle à se déresponsabiliser, pensant que l'audit externe détectera nécessairement les fraudes.

Cette situation soulève une question importante : la norme ISA 240, dans sa formulation actuelle, est-elle suffisamment explicite pour éviter ce malentendu ? La littérature académique suggère que le problème ne réside pas tant dans la clarté de la norme que dans l'écart entre les attentes légitimes des parties prenantes (expectation gap) et les capacités réelles de l'audit. Combler cet écart nécessiterait une communication plus transparente sur les limites de l'audit, mais également un renforcement de la collaboration avec les fonctions internes qui, elles, ont une mission plus explicite en matière de prévention et de détection de la fraude.

Les répondants issus de l'audit externe expriment d'ailleurs cette tension de manière récurrente. Ils reconnaissent l'importance de collaborer avec l'audit interne et la gestion des risques pour améliorer l'efficacité de leur mission, tout en insistant sur la nécessité de préserver leur indépendance et leur scepticisme professionnel. Cette tension, inhérente à la nature même de l'audit externe, n'est que partiellement abordée par la norme ISA 240, qui

se concentre davantage sur les aspects techniques de l'audit que sur les dimensions relationnelles et collaboratives.

5.2.4 COSO ERM et l'intégration du risque de fraude : de la théorie à la pratique

Le cadre COSO ERM (Enterprise Risk Management) propose une approche intégrée de la gestion des risques, où le risque de fraude devrait être identifié, évalué et géré comme tout autre risque d'entreprise, en lien avec la stratégie et les objectifs de l'organisation. Cette approche holistique suppose une coordination étroite entre la gestion des risques, l'audit interne et les autres fonctions de contrôle, ainsi qu'une intégration du risque de fraude dans les processus de gouvernance et de prise de décision.

Les résultats empiriques révèlent un écart significatif entre cette vision théorique et la réalité du terrain. Plusieurs répondants notent qu'il est plutôt rare que la fonction de gestion des risques dispose dans ses attributions la lutte contre la fraude de manière explicite. La gestion des risques est généralement responsable d'une variété de typologies de risques (financier, opérationnel, humain, légal, environnemental) sans que la fraude soit nécessairement un axe prioritaire. Cette observation suggère que l'intégration du risque de fraude dans l'ERM global, telle que préconisée par COSO, demeure largement théorique dans de nombreuses organisations.

Le témoignage de la directrice de pôle Contrôle Permanent et Risques Opérationnels dans le secteur bancaire offre toutefois un contre-exemple intéressant. Elle décrit sa fonction comme le cœur du métier en matière de lutte contre la fraude, avec une mission claire de prévenir par la cartographie et les contrôles, détecter via les indicateurs et outils de monitoring, et piloter la réponse opérationnelle. Cette approche, beaucoup plus proche de la vision COSO, illustre que l'intégration est possible, mais semble dépendre fortement du secteur d'activité (le secteur financier étant plus régulé et mature en matière de gestion des risques) et de la taille de l'organisation.

Cette variabilité soulève une question importante : le cadre COSO ERM, dans sa forme actuelle, est-il adapté aux organisations de taille moyenne qui constituent la majorité du tissu économique ? Les entretiens suggèrent que la mise en œuvre d'un ERM complet nécessite des ressources (humaines, financières, technologiques) dont ne disposent pas toutes les organisations. Dans ces contextes, le risque de fraude est souvent géré de manière fragmentée, sans l'approche intégrée préconisée par COSO, ce qui augmente le risque d'angles morts et de duplication des efforts.

5.2.5 Le contact humain face à la digitalisation

L'un des constats les plus frappants de notre étude empirique concerne l'importance accordée par les professionnels au contact humain et à la présence physique sur le terrain, et ce dans un contexte où la littérature professionnelle et académique met l'accent sur la digitalisation et l'utilisation de technologies avancées pour la détection de fraude. Ce paradoxe apparent mérite une analyse approfondie.

Les répondants insistent de manière quasi unanime sur l'importance d'"aller voir sur place" et de limiter "à outrance les échanges Teams". Cette recommandation est corroborée par les cas concrets de fraude détectés, où l'observation directe a joué un rôle déterminant. Dans le cas du détournement pour le club de football, c'est la présence physique qui a permis d'observer la tension entre le directeur financier et le directeur général, de constater la disposition des bureaux, et de repérer les éléments visuels révélateurs. Ces signaux faibles, impossibles à capter à distance, ont été décisifs pour la détection.

Parallèlement, les entretiens révèlent que l'adoption des technologies avancées (intelligence artificielle, data analytics) reste timide, freinée par des obstacles de coût, de formation et de qualité des données. Tous les répondants reconnaissent le potentiel de ces technologies, mais peu les utilisent effectivement. Cette situation semble contredire la tendance observée dans la littérature professionnelle récente, qui présente la digitalisation comme une évolution inéluctable et souhaitable de l'audit et du contrôle.

Ce paradoxe peut s'expliquer par plusieurs facteurs. Premièrement, la détection de fraude ne repose pas uniquement sur l'analyse de données quantitatives, mais également sur la perception de signaux qualitatifs (comportements, tensions, incohérences) que les technologies actuelles peinent à capter. Deuxièmement, la fraude implique souvent une dimension humaine et psychologique (le triangle de Cressey) que seule l'interaction humaine permet d'appréhender pleinement. Troisièmement, les technologies, aussi sophistiquées soient-elles, ne peuvent remplacer le jugement professionnel et le scepticisme qui sont au cœur de l'audit.

Cette observation suggère que l'avenir de la lutte contre la fraude ne réside pas dans un choix binaire entre approche humaine et approche technologique, mais dans une combinaison intelligente des deux. Les technologies peuvent améliorer l'efficacité de l'analyse de données et la détection d'anomalies quantitatives, tandis que l'observation humaine directe reste indispensable pour capter les signaux faibles qualitatifs et évaluer la culture organisationnelle. Cette complémentarité devrait être au cœur des recommandations pour une collaboration renforcée.

5.3 Propositions concrètes : Recommandations pour une collaboration renforcée

Sur la base de l'analyse critique présentée dans la section précédente et des bonnes pratiques identifiées lors des entretiens, cette section formule des recommandations concrètes visant à renforcer la collaboration entre l'audit interne, la gestion des risques et l'audit externe dans la lutte contre la fraude. Ces recommandations sont organisées selon quatre axes complémentaires : la clarification des rôles et responsabilités, la structuration de la gouvernance collaborative, l'optimisation des processus de coordination, et l'utilisation équilibrée des technologies et du contact humain.

5.3.1 5.2.1. Clarifier les rôles et responsabilités : vers une charte de collaboration antifraude

La première recommandation, fondamentale, concerne la clarification formelle des rôles et responsabilités de chaque fonction en matière de lutte contre la fraude. Comme l'ont révélé les entretiens, la confusion des rôles, particulièrement entre l'audit interne et la gestion des risques, constitue un obstacle majeur à une collaboration efficace, générant à la fois des duplications d'efforts et des angles morts.

Nous recommandons l'élaboration d'une **charte de collaboration antifraude** qui définirait de manière explicite et opérationnelle les responsabilités de chaque fonction selon les différentes phases du cycle de gestion de la fraude : prévention, détection, investigation et réponse. Cette charte devrait s'appuyer sur les référentiels professionnels existants (ISA 240, normes IIA, COSO ERM) tout en les adaptant au contexte spécifique de l'organisation.

Pour la phase de prévention, la charte pourrait préciser que la gestion des risques est responsable de l'identification et de l'évaluation du risque de fraude dans le cadre de la cartographie globale des risques, que le management opérationnel (première ligne) est responsable de la mise en œuvre des contrôles préventifs, et que l'audit interne est responsable de l'évaluation de l'efficacité de ces contrôles. L'audit externe, quant à lui, évalue l'efficacité du dispositif global dans le cadre de sa mission d'audit des états financiers.

Pour la phase de détection, la charte devrait clarifier que la gestion des risques est responsable du monitoring continu via des indicateurs de risque (KRIs) et des outils de détection automatisée, que l'audit interne est responsable de la détection lors de ses missions d'assurance, et que l'audit externe détecte les anomalies significatives dans le cadre de ses procédures d'audit. Tous les acteurs, y compris les opérationnels, ont la responsabilité de signaler les suspicions de fraude via les canaux appropriés.

Pour les phases d'investigation et de réponse, la charte devrait préciser les rôles respectifs de chaque fonction et les protocoles de coordination. L'investigation approfondie pourrait relever d'une cellule fraude dédiée ou d'experts forensic, avec un soutien de l'audit interne et de la gestion des risques. L'audit externe devrait être informé des cas de fraude significatifs et de leurs implications sur les états financiers.

Cette charte devrait être validée par le conseil d'administration ou le comité d'audit, communiquée à l'ensemble de l'organisation, et révisée périodiquement pour s'assurer de son adéquation avec l'évolution du contexte organisationnel et réglementaire.

5.3.2 5.2.2. Structurer la gouvernance collaborative : instances et mécanismes de coordination

La deuxième recommandation concerne la mise en place d'instances et de mécanismes formels de coordination entre les trois fonctions. Les entretiens ont révélé que l'absence de tels dispositifs constitue un frein majeur à une collaboration proactive, celle-ci restant souvent ponctuelle et réactive.

Nous recommandons la création d'un **comité de coordination antifraude** réunissant les responsables de l'audit interne, de la gestion des risques et, le cas échéant, un représentant de l'audit externe. Ce comité devrait se réunir à une fréquence régulière (au minimum trimestriellement) avec un ordre du jour structuré comprenant : le partage des cartographies de risques et des plans d'audit, l'examen des incidents de fraude détectés et des signalements reçus, l'évaluation de l'efficacité du dispositif antifraude global, et l'identification des zones de risque nécessitant une attention particulière ou une coordination renforcée.

Au-delà de ce comité stratégique, nous recommandons également la mise en place de mécanismes de coordination opérationnelle. Ceux-ci pourraient inclure : des réunions de lancement conjointes au début de chaque mission d'audit significative, permettant de partager les zones de risque identifiées et de coordonner les approches ; des protocoles de partage d'information en temps réel en cas de détection de signaux d'alerte ; et des revues post-mission permettant de partager les constats et les enseignements tirés.

Pour les organisations de taille moyenne ne disposant pas de ressources suffisantes pour créer des instances formelles, nous recommandons a minima la mise en place de réunions de coordination semestrielles entre les fonctions de contrôle existantes (même si certaines sont externalisées) et la direction. L'important n'est pas la sophistication du dispositif, mais la régularité et la qualité des échanges.

Ces instances de coordination devraient être soutenues par des outils de partage d'information appropriés : plateforme collaborative sécurisée, référentiel commun des risques et des contrôles, et tableaux de bord partagés. La directrice de gestion des risques interrogée recommande d'ailleurs d'"avoir un référentiel commun des contrôles et incidents relié à un outillage partagé avec des KRI homogènes". Cette recommandation souligne l'importance d'un langage commun et d'outils partagés pour faciliter la collaboration.

5.3.3 5.2.3. Optimiser les processus de coordination : de la réactivité à la proactivité

La troisième recommandation vise à transformer la nature même de la collaboration, en passant d'une approche réactive (coordination ponctuelle en cas de problème) à une approche proactive (coordination systématique et anticipative).

Nous recommandons la mise en place d'une **planification concertée des interventions** des différentes fonctions de contrôle. Concrètement, cela signifie que les plans d'audit de l'audit interne et de l'audit externe, ainsi que le plan de contrôle permanent de la gestion des risques, devraient être élaborés de manière coordonnée, en tenant compte des zones de risque identifiées par chaque fonction et en évitant les redondances inutiles. Cette planification concertée permettrait également d'identifier les zones à risque qui ne sont couvertes par aucune fonction, réduisant ainsi les angles morts.

Un professionnel de l'audit externe recommande d'ailleurs la "communication et coordination anticipative des programmes de testing de l'année". Cette pratique, observée dans certaines organisations matures, permet non seulement d'optimiser les ressources, mais aussi de renforcer la couverture globale du risque de fraude.

Au-delà de la planification, nous recommandons également la mise en place de protocoles de partage systématique des constats. Lorsque l'une des fonctions identifie une faiblesse de contrôle, un signal d'alerte ou un incident de fraude, cette information devrait être partagée rapidement avec les autres fonctions concernées, dans le respect des contraintes de confidentialité. Ce partage permettrait à chaque fonction d'adapter ses propres procédures et de renforcer la vigilance sur les zones à risque.

Nous recommandons également que l'audit externe, lorsqu'il s'appuie sur les travaux de l'audit interne conformément aux normes ISA, formalise cette utilisation dans un protocole clair précisant les modalités d'accès aux documents de travail, les critères d'évaluation de la qualité des travaux de l'audit interne, et les zones où l'audit externe pourra s'appuyer sur ces travaux. Cette formalisation permettrait de clarifier les attentes de part et d'autre et de faciliter la collaboration tout en préservant l'indépendance de l'audit externe.

5.3.4 Équilibrer technologie et contact humain : vers une approche hybride

La quatrième recommandation concerne l'utilisation équilibrée des technologies et du contact humain dans la détection de fraude. Comme l'a révélé notre analyse, ces deux approches ne sont pas antagonistes mais complémentaires, chacune apportant des capacités spécifiques que l'autre ne peut offrir.

Nous recommandons l'adoption d'une **approche hybride** combinant l'utilisation de technologies de data analytics et d'intelligence artificielle pour l'analyse quantitative et la détection d'anomalies, avec le maintien d'une présence physique régulière sur le terrain pour la perception des signaux faibles qualitatifs. Cette approche permettrait de tirer parti des forces de chaque méthode tout en compensant leurs faiblesses respectives.

Pour la dimension technologique, nous recommandons que les organisations, même de taille moyenne, investissent progressivement dans des outils de data analytics adaptés à leur contexte. Ces outils ne doivent pas nécessairement être sophistiqués ou coûteux. Des analyses réalisées via Excel ou Power BI, comme le mentionnent certains répondants, peuvent déjà apporter une valeur significative en permettant de tester des populations

complètes de transactions plutôt que des échantillons, et de détecter des anomalies qui échapperaient à une revue manuelle.

Pour les organisations plus matures, l'adoption de solutions d'intelligence artificielle peut être envisagée, mais devrait être précédée d'une évaluation rigoureuse de trois prérequis : la qualité et la disponibilité des données, les compétences des équipes pour exploiter ces outils, et l'existence d'une stratégie globale de lutte contre la fraude dans laquelle ces outils s'inscrivent. Comme le soulignent plusieurs répondants, l'IA ne peut produire de résultats fiables que si les données d'entrée sont de qualité et si les utilisateurs maîtrisent les compétences nécessaires pour interpréter les résultats.

Pour la dimension humaine, nous recommandons que les trois fonctions de contrôle maintiennent systématiquement une composante d'observation sur site dans leurs interventions, particulièrement pour les missions à risque élevé. Cette présence physique devrait être conçue non seulement comme un moyen de réaliser des contrôles, mais aussi comme une opportunité d'observer la culture organisationnelle, les relations interpersonnelles, et les signaux faibles qui ne transparaissent pas dans les documents ou les échanges virtuels.

Nous recommandons également que les réunions de coordination entre les trois fonctions privilégient le format présentiel plutôt que virtuel, particulièrement lorsqu'il s'agit de discuter de sujets sensibles ou de partager des préoccupations sur des risques de fraude. Comme le souligne un réviseur d'entreprises, il n'y a rien de tel qu'une réunion où l'on rencontre les gens pour percevoir les nuances et construire la confiance nécessaire à une collaboration efficace.

5.3.5 Renforcer la culture organisationnelle : le rôle du "tone at the top"

La cinquième et dernière recommandation concerne la dimension culturelle, souvent négligée mais pourtant fondamentale pour une collaboration efficace et une lutte efficace contre la fraude. Comme l'ont souligné de nombreux répondants, la culture organisationnelle et le "tone at the top" jouent un rôle déterminant dans l'efficacité du dispositif antifraude.

Nous recommandons que le conseil d'administration et la direction générale affirment clairement leur engagement en faveur d'une **culture de collaboration** entre les fonctions de contrôle. Cet engagement devrait se traduire par des actions concrètes : allocation de ressources suffisantes aux fonctions de contrôle, soutien visible aux initiatives de coordination, reconnaissance et valorisation des exemples de collaboration réussie, et sanction des comportements de rétention d'information ou de non-coopération.

Nous recommandons également la promotion d'une culture où le contrôle n'est pas perçu comme une remise en cause personnelle, mais comme une nécessité organisationnelle contribuant à la création de valeur. Cette transformation culturelle nécessite un travail de

communication et de sensibilisation auprès de l'ensemble de l'organisation, expliquant le rôle de chaque fonction de contrôle et l'importance de leur collaboration.

Dans le même esprit, nous recommandons le renforcement de la culture de signalement (whistleblowing). Les entretiens ont révélé que plusieurs cas de fraude ont été détectés grâce à des signalements internes. Pour encourager ces signalements, les organisations devraient mettre en place des canaux de signalement sécurisés et confidentiels, garantir la protection des lanceurs d'alerte contre les représailles, et communiquer régulièrement sur l'importance et les modalités du signalement.

Enfin, nous recommandons que les trois fonctions de contrôle organisent régulièrement des sessions de formation conjointes sur les techniques de détection de fraude, sur les normes professionnelles de chaque fonction, et sur les bonnes pratiques de collaboration. Ces formations permettraient de développer une compréhension mutuelle des rôles et des contraintes de chaque fonction, de créer des liens personnels entre les professionnels, et de renforcer la culture de collaboration.

5.4 Conclusion

Cette partie a permis de confronter les résultats empiriques de notre étude au cadre théorique établi dans les chapitres précédents, révélant des écarts significatifs entre les prescriptions normatives et la réalité du terrain. L'analyse critique a mis en lumière plusieurs constats majeurs qui éclairent la question centrale de notre recherche : comment l'audit interne, la gestion des risques et l'audit externe peuvent-ils collaborer plus efficacement pour prévenir, détecter et répondre au risque de fraude ?

Premièrement, nous avons constaté que le modèle des trois lignes de défense, bien que théoriquement clair, se heurte dans la pratique à une confusion persistante des rôles, particulièrement concernant la fonction de gestion des risques dont le périmètre varie considérablement selon les organisations. Cette confusion génère à la fois des duplications d'efforts et des angles morts dans le dispositif de contrôle, soulignant la nécessité d'une clarification formelle et contextualisée des responsabilités.

Deuxièmement, nous avons observé que le triangle de la fraude de Cressey, qui identifie la pression, l'opportunité et la rationalisation comme les trois éléments constitutifs de tout acte frauduleux, n'est appréhendé que partiellement par les fonctions de contrôle. Celles-ci se concentrent principalement sur la réduction des opportunités, négligeant largement les dimensions de la pression et de la rationalisation. Cette approche fragmentée limite l'efficacité du dispositif antifraude et plaide pour une approche plus intégrée et coordonnée.

Troisièmement, nous avons identifié un malentendu persistant concernant le rôle de l'auditeur externe en matière de fraude. Malgré la clarté de la norme ISA 240, de nombreux acteurs continuent de penser que l'audit externe a pour mission la détection de fraude. Ce malentendu crée un faux sentiment de sécurité et peut conduire à une déresponsabilisation des autres fonctions de contrôle, soulignant la nécessité d'une communication plus transparente sur les limites de l'audit et d'un renforcement de la collaboration avec les fonctions internes.

Quatrièmement, nous avons constaté que le cadre COSO ERM, qui préconise une approche intégrée de la gestion des risques incluant le risque de fraude, demeure largement théorique dans de nombreuses organisations, particulièrement de taille moyenne. Cette observation soulève la question de l'adaptabilité des référentiels professionnels aux contextes organisationnels variés et plaide pour des approches simplifiées mais structurées de la collaboration.

Cinquièmement, nous avons mis en évidence un paradoxe révélateur : alors que la littérature professionnelle met l'accent sur la digitalisation et les technologies avancées, les professionnels interrogés insistent sur l'importance irremplaçable du contact humain et de la présence physique sur le terrain. Ce paradoxe suggère que l'avenir de la lutte contre la fraude réside non dans un choix binaire entre approche humaine et approche technologique, mais dans une combinaison intelligente des deux.

Sur la base de cette analyse critique, nous avons formulé cinq recommandations concrètes et opérationnelles. La première recommande l'élaboration d'une charte de collaboration antifraude clarifiant les rôles et responsabilités de chaque fonction selon les différentes phases du cycle de gestion de la fraude. La deuxième préconise la mise en place d'instances et de mécanismes formels de coordination, adaptés à la taille et aux ressources de chaque organisation. La troisième vise à transformer la nature de la collaboration, en passant d'une approche réactive à une approche proactive basée sur la planification concertée et le partage systématique des constats. La quatrième recommande l'adoption d'une approche hybride combinant technologies et contact humain. La cinquième souligne l'importance du "tone at the top" et de la culture organisationnelle pour créer un environnement favorable à la collaboration.

Ces recommandations, ancrées dans l'expérience concrète des professionnels interrogés et éclairées par le cadre théorique, constituent autant de pistes pour renforcer la collaboration entre l'audit interne, la gestion des risques et l'audit externe. Leur mise en œuvre nécessitera un engagement fort de la direction, une allocation de ressources appropriées, et une volonté de dépasser les approches cloisonnées au profit d'une vision véritablement intégrée de la lutte contre la fraude.

La partie suivante conclura ce travail en résumant les principaux résultats, en identifiant les limites de notre étude, et en proposant des pistes pour de futures recherches dans ce domaine crucial pour la gouvernance et la pérennité des organisations.

6 Partie VI : Conclusion

Ce travail de fin d'études s'est donné pour objectif d'explorer les dynamiques de collaboration pour lutter contre la fraude : une approche intégrée entre la gestion des risques, l'audit interne et l'audit externe. Partant du constat que la fraude représente une menace croissante pour les organisations, nous avons cherché à comprendre comment ces trois fonctions peuvent collaborer efficacement malgré leurs mandats distincts et leurs contraintes spécifiques. Cette conclusion synthétise les principaux apports de notre recherche, reconnaît ses limites, propose des perspectives futures, et formule des recommandations pour renforcer cette approche intégrée.

6.1 Principales contributions du mémoire

Notre recherche apporte plusieurs contributions à la compréhension des dynamiques de collaboration dans la lutte contre la fraude.

Premièrement, ce mémoire a clarifié la nature spécifique de la contribution de chaque fonction dans une approche intégrée. L'audit interne et la gestion des risques, de par leur position interne et leur mission continue, constituent le cœur du dispositif de prévention et de détection. L'audit externe, quant à lui, apporte une contribution indirecte mais complémentaire : son indépendance, son regard externe et son expertise technique renforcent la crédibilité du dispositif global, même si sa mission première reste l'audit des états financiers et non la détection de fraude. Cette distinction est fondamentale pour comprendre les dynamiques de collaboration.

Deuxièmement, notre étude a mis en évidence un dilemme central dans les dynamiques de collaboration : la tension entre indépendance et coopération. Ce dilemme est particulièrement aigu pour l'audit externe, qui doit maintenir son scepticisme professionnel et son indépendance tout en collaborant avec les fonctions internes. Les entretiens révèlent que cet équilibre est possible à travers des protocoles clairs définissant les modalités et les limites de la collaboration, mais qu'il reste fragile et nécessite une vigilance constante. Cette tension n'est pas un obstacle insurmontable, mais une caractéristique structurelle de l'approche intégrée qu'il faut reconnaître et gérer.

Troisièmement, notre recherche a révélé que la communication constitue l'élément clé des dynamiques de collaboration efficaces. Au-delà des structures formelles et des référentiels professionnels, c'est la qualité de la communication entre les trois fonctions qui détermine l'efficacité de l'approche intégrée. Les professionnels interrogés insistent sur l'importance du contact humain direct, des réunions présentielles, et du partage systématique d'information. L'absence de communication régulière conduit à des duplications d'efforts, à des angles morts dans le dispositif de contrôle, et à une incompréhension mutuelle des rôles et contraintes de chaque fonction.

Enfin, ce mémoire a proposé des pistes concrètes pour renforcer les dynamiques de collaboration : formalisation des rôles et interfaces, création d'instances de coordination

adaptées au contexte, développement d'une culture de collaboration soutenue par le "tone at the top", et combinaison équilibrée des approches technologiques et du contact humain.

6.2 Limites du travail

Notre recherche présente certaines limites. L'échantillon, bien que diversifié, reste limité à neuf professionnels principalement basés au Luxembourg, ce qui restreint la généralisabilité des conclusions. La méthodologie qualitative, si elle permet de saisir la richesse des dynamiques collaboratives, ne permet pas de quantifier leur efficacité réelle en termes de détection de fraude. Enfin, notre étude s'est concentrée sur les perceptions des trois fonctions de contrôle, sans intégrer le point de vue du management ou des conseils d'administration, acteurs pourtant déterminants dans la création des conditions favorables à la collaboration.

6.3 Perspectives de recherche future

Ce travail ouvre plusieurs pistes pour de futures recherches. Il serait pertinent d'approfondir l'étude des dynamiques tripartites concrètes dans différents contextes organisationnels, la littérature actuelle se concentrant principalement sur les interactions binaires. La question de l'impact des technologies sur les dynamiques de collaboration mériterait également une investigation spécifique : dans quelle mesure les plateformes collaboratives et l'intelligence artificielle facilitent-elles réellement la coordination entre les trois fonctions ? Enfin, la dimension culturelle des dynamiques de collaboration pourrait faire l'objet d'études comparatives entre organisations présentant des cultures différentes.

6.4 Recommandations finales pour la profession

Au terme de ce travail, nous formulons quatre recommandations pour développer une approche véritablement intégrée de lutte contre la fraude.

Recommandation 1 : Clarifier les rôles en reconnaissant la contribution indirecte mais complémentaire de l'audit externe

Les organisations doivent formaliser les rôles de chaque fonction en reconnaissant explicitement que l'audit externe apporte une contribution indirecte à la lutte contre la fraude, complémentaire aux missions continues de l'audit interne et de la gestion des risques. Cette clarification doit définir les interfaces et les protocoles de collaboration tout en préservant l'indépendance nécessaire de l'audit externe. Une charte de collaboration peut formaliser ces rôles et gérer le dilemme entre indépendance et coopération.

Recommandation 2 : Structurer la communication entre les trois fonctions

Les organisations doivent mettre en place des mécanismes structurés de communication adaptés à leur contexte : comités de coordination pour les grandes structures, réunions semestrielles pour les organisations de taille moyenne. Ces instances doivent privilégier le contact humain direct et le format présentiel pour les sujets sensibles. La communication ne

doit pas être ponctuelle et réactive, mais régulière et proactive, incluant le partage des cartographies de risques, la coordination des plans d'intervention, et l'échange systématique des constats.

Recommandation 3 : Développer une culture de collaboration tout en préservant l'indépendance

L'approche intégrée nécessite une culture organisationnelle qui valorise le partage d'information et la transparence, tout en respectant les contraintes d'indépendance de chaque fonction. Le "tone at the top" doit clairement promouvoir cette culture de collaboration, allouer les ressources nécessaires, et reconnaître les initiatives de coordination réussies. Des formations conjointes peuvent renforcer la compréhension mutuelle des rôles, contraintes et complémentarités de chaque fonction.

Recommandation 4 : Combiner technologies et contact humain dans les dynamiques de collaboration

Les organisations doivent progressivement investir dans des outils facilitant la collaboration (plateformes partagées, référentiels communs) tout en maintenant systématiquement le contact humain direct. L'approche intégrée efficace repose sur cette combinaison : les technologies pour le partage d'information et l'analyse de données, les interactions humaines pour la construction de la confiance et la perception des signaux faibles que les outils ne peuvent capter.

En conclusion, ce mémoire a montré que les dynamiques de collaboration entre les trois fonctions constituent un levier essentiel pour une approche intégrée de lutte contre la fraude. La contribution de l'audit externe, bien qu'indirecte et complémentaire, renforce la crédibilité du dispositif global. Le dilemme entre indépendance et collaboration, loin d'être un obstacle insurmontable, peut être géré à travers des protocoles clairs et une culture de transparence. La communication régulière et de qualité constitue l'élément clé de ces dynamiques collaboratives. Dans un environnement où la fraude se sophistique, cette approche intégrée n'est plus une option, mais une nécessité pour la résilience des organisations.

7 Annexes

Les annexes présentées ci-après complètent l'analyse principale développée dans le corps du mémoire. Elles visent à documenter les outils méthodologiques mobilisés, à apporter des précisions sur la démarche empirique et à renforcer la transparence scientifique du travail.

Elles comprennent notamment :

- Les guides d'entretien utilisés auprès des professionnels interrogés
- Un tableau descriptif des participants ayant accepté de contribuer
- Les transcriptions intégrales des entretiens réalisés

Ces annexes contribuent à la rigueur méthodologique de l'étude et garantissent la fidélité du processus de recherche mené.

Annexe 1 : Guide d'entretien

Objectif du guide

Le présent guide a été élaboré pour structurer les entretiens semi-directifs réalisés auprès de professionnels évoluant dans les fonctions d'audit interne, de gestion des risques et d'audit externe en Belgique, en France, au Luxembourg et au Maroc.

L'objectif est de recueillir leur perception et leur expérience concernant les dynamiques de collaboration entre ces trois fonctions dans le cadre de la lutte contre la fraude. Plus spécifiquement, nous cherchons à comprendre comment ces acteurs coordonnent leurs efforts, partagent l'information, définissent leurs responsabilités respectives et surmontent les défis organisationnels qui peuvent entraver une approche intégrée de la prévention et de la détection de la fraude.

Le guide explore également les facteurs qui facilitent ou freinent cette collaboration, l'impact des nouvelles technologies sur ces interactions, ainsi que les perspectives d'évolution de ces relations professionnelles dans un environnement réglementaire en constante mutation.

Le guide a été conçu de manière flexible afin de permettre des approfondissements selon les réponses des participants et leur domaine d'expertise spécifique.

Questions posées

Questions
1. Informations générales et contexte professionnel
Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
Depuis combien d'années travaillez-vous dans ce domaine ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenu ?
2. Perception des rôles et responsabilités
Comment définiriez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
Selon vous, quelles sont les responsabilités clés respectives de l'audit interne, de l'audit externe et de la gestion des risques dans ce domaine ?
Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ? Si oui, sur quels aspects ?
La responsabilité en matière de détection de la fraude est-elle suffisamment claire dans votre organisation ? Pourquoi ?
3. Références normatives et professionnalisme
Connaissez-vous les exigences de la norme ISA 240 ? Si oui, comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
L'audit interne est-il, selon vous, positionné de manière stratégique pour jouer pleinement son rôle dans la lutte contre la fraude, tel que défini par les normes de l'IIA notamment en matière d'évaluation du contrôle interne, de conseil au management et de coordination avec les autres fonctions ?
Des divergences d'interprétation sur la mission de l'auditeur externe dans la détection de la fraude nuisent-elles, selon vous, à la collaboration interfonctionnelle ?
4. Collaboration et coordination entre fonctions
À quelle fréquence travaillez-vous en coordination avec les autres fonctions de contrôle (audit interne, gestion des risques, audit externe) ?
Existe-t-il dans votre organisation des dispositifs formels de coordination entre les fonctions (ex. : comités, plans d'audit concertés, réunions croisée) ?
Comment qualifieriez-vous la qualité actuelle de la collaboration entre ces trois fonctions dans votre organisation (ou dans les organisations que vous connaissez) ?

Quels sont, selon vous, les principaux freins à une collaboration efficace ? (culturels, structurels, liés à la gouvernance, à la confidentialité, etc.)
Quels facteurs ou leviers facilitent une synergie réussie entre ces fonctions ?
5. Méthodologies, outils et partage d'information
Quels outils ou techniques utilisez-vous pour identifier, évaluer ou détecter des risques de fraude ?
Partagez-vous ces résultats ou données avec d'autres fonctions de contrôle ? Si oui, par quels canaux ?
Existe-t-il des processus formalisés de partage de l'information liée à la fraude entre audit interne, audit externe et gestion des risques ?
Observez-vous un risque de redondance ou de duplication dans les efforts de détection ou d'audit ? Si oui, comment cela pourrait-il être évité ?
6. Rôle de l'intelligence artificielle et technologies
Votre organisation utilise-t-elle des outils de data analytics ou d'IA pour détecter des comportements frauduleux ?
Selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer la collaboration entre audit interne, audit externe et gestion des risques ?
Quelles sont les principales limites à l'adoption de ces technologies dans votre domaine (coût, formation, manque de stratégie, etc.) ?
7. Bonnes pratiques et recommandations
Connaissez-vous des exemples de bonnes pratiques ou de modèles de collaboration réussie dans la lutte contre la fraude ? (dans votre organisation ou ailleurs)
Si vous deviez formuler une recommandation pour améliorer la collaboration interfonctionnelle, quelle serait-elle ?
Selon vous, quel rôle la culture organisationnelle joue-t-elle dans la réussite (ou l'échec) d'une stratégie antifraude intégrée ?

Remarques :

- Lors de l'entretien, l'ordre des questions pouvait être légèrement adapté selon le déroulé naturel de la conversation et la fonction spécifique du participant.
- En fonction des contraintes horaires et de l'expertise particulière de chaque répondant, seules les questions jugées les plus appropriées et nécessaires ont été posées, permettant ainsi d'optimiser le temps d'échange tout en respectant la disponibilité des professionnels interrogés.
- Les participants étaient libres de développer certains points plus en profondeur ou d'illustrer leurs réponses par des exemples pratiques tirés de leur expérience professionnelle.
- Certains axes thématiques ont pu être privilégiés selon que l'interviewé évoluait principalement dans l'audit interne, la gestion des risques ou l'audit externe, afin de tirer parti de son expertise spécifique dans ces domaines.

Annexe 2 : Tableau descriptif des participants aux entretiens

Objectif

Ce tableau présente de manière synthétique et anonymisée les principales caractéristiques des participants aux entretiens réalisés dans le cadre de l'étude empirique. Il vise à illustrer la diversité des profils interrogés tout en respectant la confidentialité des personnes et des structures.

Code du Participant	Sexe	Fonction Exercée	Expérience professionnelle (années)	Type de Cabinet
PA1	Homme	Réviseur d'entreprise Agrée	29 Ans	Cabinet Local
PB2	Homme	Réviseur d'entreprise Agrée	13 Ans	Cabinet Local, Ex Grand Cabinet
PC3	Homme	Senior Manager Audit Externe	13 Ans	Cabinet Local
PD4	Femme	Manager Audit Externe	6 Ans	Grand Cabinet
PE5	Femme	Manager Audit Externe	8 ans	Cabinet Local
PF6	Homme	Réviseur d'entreprise (Mandats Audit Interne)	5 Ans	Cabinet Local
PG7	Homme	Partner, Business Risk Services (Audit Interne)	11 Ans	Grand Labinet
PH8	Homme	Manger Audit Interne	5 Ans	Société Cotée
PI9	Femme	Directrice département Contrôle Permanent et Risque Opérationnel	13 ans	Société Cotée

Annexe 3 : Entretien 1 : Réviseur d'entreprise Agrée, Code : PA1

Question : Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
PA1 : je suis Réviseur d'entreprises agréé signataire des missions d'audit des états financiers
Question : Depuis combien d'années travaillez-vous dans ce domaine ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
PA1 : Actif depuis 29 ans dans le métier d'audit. Passé tous les grades de junior à associé
Question : Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenu ?
PA1 : Non, nous n'avons pas eu de cas de fraude au cours des 5 dernières années
Question : Comment définiriez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
PA1 : Comme REA, nous devons être attentifs pour des cas et/ou indications de fraude et les analyser et rapporter quand on les découvre. Notre mission n'est pas d'investiguer spécifiquement sur la fraude mais de rester vigilants.
Question : Selon vous, quelles sont les responsabilités clés respectives de l'audit interne, de l'audit externe et de la gestion des risques dans ce domaine ?
PA1 : Audit interne càd monitoring des procédures de contrôle interne sur set up et exécution càd procédures plus larges que les contrôles internes liés à la préparation des états financiers.
Audit externe càd de un identifier les procédures de contrôle interne (dont fraude et management override) en lien avec la préparation des états financiers, de deux tester et évaluer leur efficacité, de trois rapporter les conclusions/avis au management, de quatre décider de s'appuyer ou non sur les contrôles internes dans l'audit des états financiers. Plus les contrôles internes sont efficaces, moins le risque d'audit reste à couvrir.
Question : Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ? Si oui, sur quels aspects ?
PA1 : Dans les grandes entreprises, cette distinction est suffisamment claire.
Question : La responsabilité en matière de détection de la fraude est-elle suffisamment claire dans votre organisation ? Pourquoi ?
PA1 : Oui, suffisamment claire. Parce que très peu de dossiers ont un service de contrôle interne actif.
Question : Connaissez-vous les exigences de la norme ISA 240 ? Si oui, comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
PA1 : Oui.
Question : L'audit interne est-il, selon vous, positionné de manière stratégique pour jouer pleinement son rôle dans la lutte contre la fraude, tel que défini par les normes de l'IIA notamment en matière d'évaluation du contrôle interne, de conseil au management et de coordination avec les autres fonctions ?
PA1 : Oui, dans la mesure où les principes d'indépendance et d'objectivité du service de contrôle interne sont assurés.
Question : Des divergences d'interprétation sur la mission de l'auditeur externe dans la détection de la fraude nuisent-elles, selon vous, à la collaboration interfonctionnelle ?
PA1 : Cela dépend de la façon dont le service de contrôle interne fonctionne. Le mieux est qu'il fonctionne comme s'il n'y avait pas d'audit externe et couvre tous les aspects.
Question : À quelle fréquence travaillez-vous en coordination avec les autres fonctions de contrôle (audit interne, gestion des risques, audit externe) ?

PA1 : Très rarement, car nous avons presque aucun client avec un service de contrôle interne opérationnel.
Question : Quels outils ou techniques utilisez-vous pour identifier, évaluer ou détecter des risques de fraude ?
PA1 : Tests sur procédures de contrôle interne / interviews management / JET Testing
Question : Votre organisation utilise-t-elle des outils de data analytics ou d'IA pour détecter des comportements frauduleux ?
PA1 : Non
Question : Selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer la collaboration entre audit interne, audit externe et gestion des risques ?
PA1 : Traitement rapide d'un volume de données. Échange d'informations entre les différents services.
Question : Quelles sont les principales limites à l'adoption de ces technologies dans votre domaine (coût, formation, manque de stratégie, etc.) ?
PA1 : Coût et formation
Question : Si vous deviez formuler une recommandation pour améliorer la collaboration interfonctionnelle, quelle serait-elle ?
PA1 : Communication et coordination anticipative des programmes de testing de l'année.
Question : Selon vous, quel rôle la culture organisationnelle joue-t-elle dans la réussite (ou l'échec) d'une stratégie antifraude intégrée ?
PA1 : Si le management est "control minded", une stratégie antifraude intégrée a plus de chances de bien fonctionner.

Annexe 4 : Entretien 2 : Réviseur d'entreprise Agrée, Code : PB2

AZ : Donc la première question, c'est juste pour des informations générales. Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
PB2 : Bah donc tu connais. Je suis réviseur d'entreprise ici, réviseur d'entreprise agréé ici.
AZ : Et depuis combien de temps travaillez-vous dans le domaine de l'audit surtout ?
PB2 : 13 ans.
AZ : Et donc, votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenu ? Quand je dis votre organisation, soit les entreprises dans lesquelles vous avez travaillé, soit les clients.
PB2 : Donc ta question, c'est de savoir, est-ce que j'ai déjà été confronté à des cas de fraude sur un des mandats ?
AZ : Oui, exactement. Soit en interne, soit en externe.
PB2 : En interne, c'est-à-dire ?
AZ : dans l'entreprise.
PB2 : Ah, en entreprise ? Non. Mais chez les clients, oui. Et la fréquence, par exemple, si on a un pourcentage ? Ah, écoute, c'est ce que l'auditeur redoute le plus. Donc, moins ça se produit, mieux c'est. Mais moi, j'ai en tête deux mandats sur 13 ans, donc ça va. Mais encore une fois, lorsque c'est avéré, c'est ça le dilemme.
AZ : Et donc, comment définissez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
PB2 : Alors, aucune, parce qu'il y a un grand principe d'indépendance qui régit notre profession. Et donc, on n'est pas là pour ni anticiper, ni détecter, ni corriger les cas de fraude. D'accord ? On est là uniquement pour s'assurer que si on émet une opinion qui atteste de l'image sincère des états financiers, que cette image sincère soit exempte d'anomalies significatives provenant de fraudes ou d'erreurs. C'est le seul cadre de notre intervention. Et donc, effectivement, on n'est pas là pour aider le client à mettre les mesures qui s'imposent en place, on est là pour s'assurer qu'il a fait son travail.
AZ : Et donc, en revenant sur cela, selon vous, quelles sont les responsabilités clés respectives de l'audit interne et du département de gestion du risque ?
PB2 : Pour moi, il y a deux. Bon, entre les aspects théoriques, comme tu as dit, prévention, etc. Pour moi, il y a deux principes clés. Alors, le principe clé pour moi déjà, c'est la bonne gouvernance. D'accord ? C'est le tone at the top, le message que donne la direction. C'est ça qui fait que dès lors où il y a les bons principes de gouvernance en place, on réduit de manière importante les risques de fraude. Ensuite, pour moi, il y a le principe clé de séparation des tâches, d'accord ? Qui va, de fait, avec un bon principe de bonne gouvernance. Et surtout, la compétence, c'est-à-dire mettre les bonnes personnes aux bons endroits. Donc, dans une organisation, être certain que chaque personne ait les tâches qui conviennent le mieux à leur compétence. Et c'est grâce à ça que, déjà, on évite les cas d'erreur, mais aussi de fraude.
AZ : Donc, là, je vais passer à une autre partie qui s'appelle la méthodologie outils et partage d'informations. Donc, quels outils techniques utilisez-vous dans le cadre de la fraude en étant un réviseur d'entreprise ? Soit dans vos tests, soit dans...
PB2 : Alors, moi, j'ai toujours connu des méthodes assez artisanales, d'accord ? Que ce soit ici ou même dans les big four, parce qu'à l'époque, l'intelligence artificielle n'était pas spécialement exploitée ou n'existait pas, en fait. Mais, en fait, de manière générale, c'est toujours ça le dilemme, c'est jusqu'où on doit aller, quel degré de détail on doit aller pour essayer de s'assurer que nos diligences soient remplies. Donc, je pense qu'encore une fois,

la principale base, c'est quand même de discuter avec les responsables du gouvernement d'entreprise, comment eux perçoivent la chose. Et je pense que c'est ça le socle qui va tailor nos procédures d'audit. C'est-à-dire, quand on est dans un... Ça, c'est déjà arrivé, dans un environnement de contrôle très faible ou avec une intégrité de la direction qui peut être remise en question, là, effectivement, il faut aller plus loin dans les démarches. Et pour te donner un exemple, moi, j'ai déjà eu le cas où on a fait intervenir des équipes forensiques parce qu'on avait des grosses suspicions dues, justement, à l'intégrité de la direction. Donc, tout dépend, encore une fois, des procédures d'audit, dépend de la perception que l'auditeur peut avoir d'un environnement de contrôle et de l'intégrité de la direction. Après, effectivement, il y a de plus en plus les outils technologie et intelligence artificielle qui peuvent nous aider à, j'ai envie de dire, à orienter au mieux nos procédures. Mais ça reste toujours du jugement.
AZ : Donc, en rebondissant sur ce point exactement, moi, j'ai mis une partie rôle de l'intelligence artificielle des technologies. J'ai deux questions. La première, est-ce que votre organisation utilise-t-elle des outils de data analytics ou d'IA ? Et la deuxième question est que, selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer soit la collaboration entre les trois fonctions, si elles existent, avec des limites, bien sûr, ou bien pour chaque fonction indépendamment ?
PB2 : Alors, première réponse, première question, non. Malheureusement, on va commencer à se pencher sur la question. C'est l'utilisation de l'intelligence artificielle dans les procédures d'audit, que ce soit de fraude ou d'ailleurs. Pour le moment, ce n'est pas le cas. Deuxième question. Alors, l'interaction... Deuxième question, il y a deux volets. C'est l'interaction entre les trois fonctions. Pour moi, l'intelligence artificielle ne va pas spécialement aider à mieux communiquer ou à mieux comprendre. Je ne pense pas que ça va aider. Par contre, effectivement, dans l'audit, l'intelligence artificielle, dans les procédures d'audit liées à la fraude, peuvent être très intéressantes parce que même si... Tu sais qu'il y a... Au reste des humains, le risque d'erreur à notre niveau existe. L'intelligence artificielle permet, je pense, de peut-être combler certaines lacunes et peut-être d'avoir une vision peut-être plus objective par rapport à ce qu'on pourrait avoir. Donc, l'intelligence artificielle, surtout dans le cas de la fraude, elle permet, je pense, d'améliorer l'efficacité des procédures. Ça, c'est très clair.
AZ : Donc, pour moi, je vais vous poser une dernière question. Donc, si vous devez formuler une recommandation pour améliorer la collaboration interfonctionnelle, quelle serait-elle ? On sait très bien que maintenant, ce n'est pas le cas, mais si vous avez une idée de... Par exemple...
PB2 : Alors, déjà, la première chose, c'est très basique, mais c'est de limiter à outrance... Enfin, de stopper les échanges Teams à outrance. C'est très bête, mais il n'y a rien de tel qu'une réunion où tu rencontres les gens ou justement, tu viens te rendre compte des processus sur place. Ça, ça ne remplacera jamais. Et donc, ça, c'est déjà une piste que moi, je trouve, c'est... Voilà. Les outils technologiques, notamment de communication, ont souvent leurs limites. Et il faut revenir à... C'est peut-être un peu vieille école, mais... À des procédures beaucoup plus terre-à-terre. Ou voilà, si moi, je dois intervenir sur un client où il y a une direction opérationnelle, un département d'audit interne, un département de gestion des risques, c'est justement de discuter avec eux, de voir quelles sont leurs procédures mises en place de manière très concrète. Ce qui ne peut être fait, à mon sens, que si on va voir les principales personnes concernées. Il ne faut pas oublier que tout ça, ça reste quand même de la discussion, de la compréhension, et que ça se perçoit beaucoup

mieux quand c'est en live, en direct, plutôt que par des échanges Teams. Ou là, justement, on perçoit moins bien les choses.
PB2 : Parce que je vais donner un exemple très concret. En fait, un des cas de fraude avec lesquels j'ai été confronté, c'est le directeur d'une société qui utilisait des fonds de cette société-là pour les besoins de son club. Comment ça s'est matérialisé, ça ? Il y a le CFO qui, un jour, nous a appelés en disant vous devez faire très attention aux notes de frais et aux dépenses qui ne sont pas tout le temps liées à l'activité. Et donc, avec cette information-là, qu'est-ce qu'on va faire ? On s'est dit OK, mais on va aller voir sur place. D'accord ? De manière neutre. Déjà, en allant sur place, ce qu'on a constaté, c'est qu'il y avait une tension très palpable entre ce CFO et ce directeur général. D'accord ? Ça s'est vu tout de suite dans les échanges, dans la manière où le bureau était positionné, le gars était à l'autre bout. Et on a tout de suite senti, en disant OK, mais il y a une allégation ici de quelqu'un qui a quelque chose envers cette personne-là. Donc, on s'est dit, est-ce qu'on donne du sens à l'information qu'il nous a donnée ou pas ? Après, en allant sur place, effectivement, ce qu'il nous avait donné comme information, il nous avait cité un club de foot très précis. Effectivement, en allant sur place, on a vu que ce gars-là avait les chartes du club, avait une photo, et en ayant été sur la photo, parce qu'on avait fait des recherches sur Internet, on a effectivement vu qu'il faisait partie de l'équipe. Il était, en fait, je pense qu'il était trésorier ou je ne sais pas quoi. Et donc, tout ça pour te dire que dans des cas comme ça qui sont parfois très délicats, rien de tel que d'aller voir sur place et voir, effectivement, si certaines informations peuvent être corroborées ou pas par rapport à ce qu'on peut voir sur Internet, par rapport à ce qu'on peut entendre ou lire sur Google. Et donc, ça, c'est un exemple qui me fait dire que oui, c'est en allant voir les personnes concernées, les processus qu'on peut se rendre compte. C'était le cas. Il y avait effectivement des grosses problématiques, des détournements.
AZ : Peut-être sur ça, une autre petite question. Est-ce que, par exemple, l'auditeur a une obligation de reporter à un organisme spécifique ?
PB2 : Bien sûr.
AZ : Par exemple, le Luxembourg.
PB2 : Oui. Donc, tu as la CRF. Donc, c'est la cellule de renseignement financier où, effectivement, ils parlent des infractions de premier degré à reporter à la CRF. L'infraction de premier degré, tu as une liste. Donc, en gros, dans cette liste-là, il y a marqué fraude. Donc, tu es censé remonter au parquet. Tout cas avéré de fraude à la CRF. D'accord ? Ensuite, s'il y a aussi une... Il y a quand même une possibilité qui est donnée à l'auditeur de démissionner pour juste motif. Et, effectivement, l'intégrité de la direction, selon l'ISA 240, peut être évoquée comme un juste motif qui peut mettre fin à la relation contractuelle. Et dans ce cas-là, il faut intervenir à la CSSF si c'est un audit légal en disant qu'on démissionne de ce mandat-là. En tant qu'auditeur légal, en tant qu'auditeur réviseur d'entreprise agréé de cette société-là, on démissionne pour telle raison. Donc, voilà, il y a déjà deux organismes à informer. Alors, quand c'est les assurances, c'est le commissariat aux assurances. Bien entendu, au cas de fraude, outre les externes, en interne, ça doit être communiqué, comme ils disent, de manière pertinente.
AZ : Et bien, voilà, c'était toutes mes questions. Merci beaucoup.
PB2 : Je t'en prie. Merci.

Annexe 5 : Entretien 3 : Senior Manager Audit Externe, Code : PC3

PC3 : Je suis Senior Manager dans un cabinet d'audit, je supervise plusieurs dossiers et j'ai une fonction d'associé dans l'organisation interne. J'ai environ 13 ans d'expérience dans ce domaine, ce qui me permet d'avoir une vision assez complète des enjeux. Mon rôle consiste principalement à encadrer les équipes sur les missions, à valider les approches d'audit et à maintenir les relations avec les clients. Je m'occupe aussi de la formation des plus juniors.
AZ : Depuis combien d'années travaillez-vous dans ce domaine ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
PC3: Comme je le disais, ça fait 13 ans maintenant. J'ai commencé comme auditeur junior, puis j'ai évolué vers senior, manager, et maintenant senior manager. Cette progression m'a donné une perspective intéressante sur l'évolution du métier et des relations avec les autres fonctions de contrôle.
AZ: Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenu ?
PC3 : Oui, il y a 5 ans on a eu un cas de fraude assez significatif. C'était lié à la carte bancaire pour des besoins personnels, donc un détournement classique mais qui avait pris de l'ampleur. Mon rôle a été de coordonner l'investigation et de m'assurer que nos procédures d'audit étaient adaptées pour détecter ce type d'irrégularités à l'avenir.
AZ : Comment définissez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
PC3 : Au niveau des clients, on n'est pas forcément là pour auditer la fraude, mais on intervient quand même dans ce processus. Notre rôle principal reste l'audit des comptes, mais on a une responsabilité de vigilance. Quand on détecte des anomalies ou des signaux faibles, on doit creuser et alerter si nécessaire.
AZ : Selon vous, quelles sont les responsabilités respectives de l'audit interne, de l'audit externe et de la gestion des risques dans ce domaine ?
PC3 : C'est une bonne question parce que les frontières ne sont pas toujours claires. L'audit interne est plus dans le préventif et le suivi continu, nous on arrive avec un regard externe ponctuel, et la gestion des risques fait le lien entre les deux.
AZ : Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ? Si oui, sur quels aspects ?
PC3 : Oui, ça dépend du client effectivement. Dans certaines organisations, les rôles sont bien définis, mais dans d'autres, on voit que l'audit interne fait parfois du travail qu'on pourrait considérer comme relevant de la gestion des risques, ou inversement. Et nous, en tant qu'auditeurs externes, on peut parfois empiéter sur leurs domaines quand on identifie des faiblesses de contrôle interne.
AZ : Connaissez-vous les exigences de la norme ISA 240 ? Si oui, comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
PC3 : Oui bien sûr, la responsabilité de l'auditeur doit être de garder un œil sceptique professionnel. On doit maintenir une attitude de scepticisme tout au long de la mission et adapter nos procédures quand on identifie des risques de fraude. Mais il faut être clair : on n'est pas des détectives, on fait de l'audit.
AZ : L'audit interne est-il, selon vous, positionné de manière stratégique pour jouer pleinement son rôle dans la lutte contre la fraude, tel que défini par les normes de l'IIA notamment en matière d'évaluation du contrôle interne, de conseil au management et de coordination avec les autres fonctions ?

PC3 : Théoriquement oui, mais dans la pratique, ça dépend vraiment de l'organisation. Certains audits internes ont une vraie indépendance et peuvent jouer ce rôle stratégique, d'autres sont plus limités par leur positionnement hiérarchique ou leurs ressources.
AZ : À quelle fréquence travaillez-vous en coordination avec les autres fonctions de contrôle (audit interne, gestion des risques, audit externe) ?
PC3 : Aucune fonction audit interne, on évalue le contrôle interne. On se fie pas au contrôle sur place. L'inexistence cause problème. En fait, quand il n'y a pas d'audit interne, c'est plus compliqué pour nous parce qu'on doit faire plus de travail substantif. Quand il y en a un, on peut s'appuyer sur leurs travaux, mais on garde notre indépendance.
AZ : Quels facteurs ou leviers facilitent une synergie réussie entre ces fonctions ?
PC3 : Si l'auditeur externe existe, ça facilite le dialogue dès le début de la mission et en cours. Oui, bien sûr, si l'audit interne et la gestion des risques sont bien structurés, ça nous aide énormément. On peut échanger sur les zones de risque, partager certaines informations, et éviter de refaire le même travail. La communication est vraiment la clé.
AZ : Votre organisation utilise-t-elle des outils de data analytics ou d'IA pour détecter des comportements frauduleux ?
PC3 : Pas forcément, plus la taille et le coût. On commence à utiliser des outils d'analyse de données, mais c'est encore limité par les coûts et la complexité de mise en œuvre. Pour les petites missions, c'est pas toujours rentable.
AZ : Selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer la collaboration entre audit interne, audit externe et gestion des risques ?
PC3 : Ça pourrait faciliter les contrôles, permettre d'analyser un plus grand nombre de données, vérifier la ségrégation, faire des analyses poussées sur des mouvements suspects. L'IA pourrait nous aider à identifier des patterns qu'on ne verrait pas forcément à l'œil nu et à partager ces informations plus facilement entre les différentes fonctions.
AZ : Quelles sont les principales limites à l'adoption de ces technologies dans votre domaine (coût, formation, manque de stratégie, etc.) ?
PC3 : La qualité du client et du besoin principalement. Il faut que le client ait des données de qualité et soit prêt à investir dans ces technologies. Et de notre côté, il faut former les équipes, ce qui représente un coût et du temps.
AZ : Selon vous, quel rôle la culture organisationnelle joue-t-elle dans la réussite (ou l'échec) d'une stratégie antifraude intégrée ?
PC3 : C'est fondamental. Quand on a plusieurs personnes, on se base sur la confiance qui peut biaiser la chaîne de contrôle. Il faut plus de reliance sur celui qui contrôle en amont ou en aval. La culture doit promouvoir la transparence et accepter que le contrôle ne soit pas une remise en cause personnelle, mais une nécessité organisationnelle.

Annexe 6 : Entretien 4 : Manager Audit Externe, Code : PD4

AZ : Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
PD4 : Je suis actuellement manager en audit externe, en charge de différents clients. Le rôle de manager est d'encadrer les équipes d'audit tout au long de l'audit. Cela passe par l'établissement du planning, le contact avec le client, l'identification des risques de chaque client, l'établissement de la stratégie d'audit, la revue des travaux préparés par l'équipe, la conclusion de l'audit, l'archivage des dossiers. Il y a l'aspect financier également, tel qu'établir les budgets d'audit, en discuter avec le client, veiller à ce que le budget d'audit soit respecté, vérifier les timesheets des équipes. Dernièrement, il y a tout ce qui est interne à l'entreprise tel que le développement des formations internes, les évaluations ponctuelles et annuelles des équipes d'audit, etc.
AZ : Depuis combien d'années travaillez-vous dans ce domaine ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
PD4 : Cela fait 6 ans que je travaille dans ce domaine. J'ai commencé chez Deloitte Luxembourg en tant que stagiaire en 2019, puis junior 1, 2, senior 1, 2, 3 et enfin manager. Cette évolution m'a donc permise de commencer par des tests d'audit spécifiques tels que les tests de cash, puis d'approfondir et élargir mes connaissances et compétences, jusqu'à pouvoir gérer un audit de A à Z.
AZ : Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenu ?
PD4 : Non, pas à ma connaissance.
AZ : Comment définiriez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
PD4 : En tant qu'auditeur externe, nous sommes règlementés par la norme ISA 240 qui décrit notre responsabilité face à la fraude. Pour ce qui est de la prévention de la fraude, nous n'en sommes pas responsables il me semble. Cependant, le fait que nous pouvons émettre une lettre de recommandation (management letter), si nous identifions des défaillances dans les contrôles ou l'environnement de l'entité auditée, cela pourrait être vu comme une prévention de la fraude. En ce qui concerne la détection, cela n'est pas notre responsabilité. Cependant, nous devons établir des procédures d'audit face au risque de fraude. Pour la gestion de la fraude, si nous détectons une fraude, il est de notre ressort d'en avertir les personnes compétentes.
AZ : Selon vous, quelles sont les responsabilités clés respectives de l'audit interne, de l'audit externe et de la gestion des risques dans ce domaine ?
PD4 : Pour moi, l'audit interne sert à vérifier les contrôles en place au sein d'une entreprise. Ces contrôles sont mis en place afin de prévenir et détecter la fraude, mais aussi les erreurs. L'audit interne joue donc un rôle en termes de prévention et détection de la fraude. Pour ce qui est de l'audit externe, nous n'avons pas la responsabilité de détecter la fraude. Notre responsabilité est de s'assurer que les états financiers reflètent la réalité économique de l'entité auditée. Nous avons la responsabilité de détecter toutes différences significatives, provenant de la fraude ou de l'erreur.
AZ : Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ? Si oui, sur quels aspects ?
PD4 : En tant qu'auditeur, non. Cependant, je pense que parfois les clients ou des personnes externes au métier pourraient penser que notre rôle est la détection de la fraude.
AZ : La responsabilité en matière de détection de la fraude est-elle suffisamment claire dans votre organisation ? Pourquoi ?

PD4 : Il me semble que oui. Nous abordons le sujet de la fraude dans chacun de nos meetings en début d'audit. De plus, ce sujet est également abordé lors des formations organisées en interne.
AZ : Connaissez-vous les exigences de la norme ISA 240 ? Si oui, comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
PD4 : Oui, j'ai connaissance de la norme ISA 240.
AZ : L'audit interne est-il, selon vous, positionné de manière stratégique pour jouer pleinement son rôle dans la lutte contre la fraude, tel que défini par les normes de l'IIA ?
PD4 : N'ayant pas un background en audit interne, je ne connais pas les normes IIA. Cependant, je pense que l'audit interne a un rôle important dans la lutte contre la fraude.
AZ : Des divergences d'interprétation sur la mission de l'auditeur externe dans la détection de la fraude nuisent-elles, selon vous, à la collaboration interfonctionnelle ?
PD4 : Oui, cela pourrait nuire dans le cas où le management penserait que l'auditeur externe est responsable de la détection de la fraude et lui 'renverrait la balle'.
AZ : À quelle fréquence travaillez-vous en coordination avec les autres fonctions de contrôle (audit interne, gestion des risques, audit externe) ?
PD4 : Très rarement.
AZ : Existe-t-il dans votre organisation des dispositifs formels de coordination entre les fonctions (ex. : comités, plans d'audit concertés, réunions croisées) ?
PD4 : Pas à ma connaissance.
AZ : Comment qualifieriez-vous la qualité actuelle de la collaboration entre ces trois fonctions dans votre organisation ?
PD4 : Je n'ai pas connaissance de collaboration spécifique entre ces trois fonctions dans mon organisation.
AZ : Quels sont, selon vous, les principaux freins à une collaboration efficace ?
PD4 : Confidentialité, séparation des tâches et des responsabilités.
AZ : Quels facteurs ou leviers facilitent une synergie réussie entre ces fonctions ?
PD4 : La communication claire – le partage clair des responsabilités.
AZ : Quels outils ou techniques utilisez-vous pour identifier, évaluer ou détecter des risques de fraude ?
PD4 : Nous avons deux risques de fraude en audit externe : Management override of control : nous examinons les contrôles en place dans l'entreprise concernant l'enregistrement des entrées comptables. Nous effectuons ensuite le 'jet testing', qui consiste à scruter le grand livre et à s'assurer qu'aucune transaction 'en dehors de l'activité normale' de l'entité n'a eu lieu. Revenue recognition : dans les fonds d'investissement, qui représentent la majorité de mon portefeuille, nous réfutons ce risque de fraude car le revenu n'est pas complexe, il est sur base de contrat et la fraude peut difficilement s'y installer. Nous discutons également lors du TPM de chaque client de la fraude avec les équipes d'audit. Dernièrement, nous faisons remplir un questionnaire fraude aux responsables de la gouvernance de l'entité auditée.
AZ : Partagez-vous ces résultats ou données avec d'autres fonctions de contrôle ? Si oui, par quels canaux ?
PD4 : Non.
AZ : Existe-t-il des processus formalisés de partage de l'information liée à la fraude entre audit interne, audit externe et gestion des risques ?
PD4 : Pas à ma connaissance.

AZ : Observez-vous un risque de redondance ou de duplication dans les efforts de détection ou d'audit ? Si oui, comment cela pourrait-il être évité ?
PD4 : Pas à ma connaissance.
AZ : Votre organisation utilise-t-elle des outils de data analytics ou d'IA pour détecter des comportements frauduleux ?
PD4 : Pas à ma connaissance.
AZ : Selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer la collaboration entre audit interne, audit externe et gestion des risques ?
PD4 : Non pas forcément, je pense que la collaboration doit être améliorée par les humains. Par contre, l'intelligence artificielle peut aider chaque fonction séparément.
AZ : Quelles sont les principales limites à l'adoption de ces technologies dans votre domaine (coût, formation, manque de stratégie, etc.) ?
PD4 : Coût, formation.
AZ : Selon vous, quel rôle la culture organisationnelle joue-t-elle dans la réussite (ou l'échec) d'une stratégie antifraude intégrée ?
PD4 : La culture organisationnelle joue un rôle important dans la stratégie antifraude. Si les équipes sont impliquées, qu'elles savent pourquoi c'est important, que c'est bien organisé, il sera plus facile de détecter ou éviter la fraude. Également, la culture de l'entreprise joue un rôle important dans l'opportunité, l'intention et la rationalisation de la fraude.

Annexe 7 : Entretien 5 : Manager Audit Externe, Code : PE5

AZ : Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
PE5 : Je suis manager en audit externe depuis plusieurs années. Mon rôle consiste à superviser les missions d'audit légal et contractuel, à coordonner les équipes d'auditeurs et à assurer la qualité des travaux réalisés. J'interviens également dans la communication des résultats d'audit auprès des clients et dans la formulation de recommandations sur le contrôle interne.
AZ: Depuis combien d'années travaillez-vous dans le domaine de l'audit externe ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
PE5: Cela fait neuf ans que je travaille dans le domaine de l'audit. J'ai toujours exercé en audit externe, sans changement de fonction vers l'audit interne ou la gestion des risques.
AZ : Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenue ?
PE5 : Pas au cours des cinq dernières années, mais lorsque j'étais junior, j'ai travaillé sur un dossier où une société avait mis en place une pyramide de Ponzi. Nous avions relevé des indicateurs suspects, et après des recherches sur Internet, nous avons trouvé des articles confirmant l'existence du schéma frauduleux. Nous avons alors transmis l'information à la cellule spécialisée au Luxembourg.
AZ : Selon vous, quelles sont les responsabilités clés respectives de l'audit interne, de l'audit externe et de la gestion des risques dans le domaine de la lutte contre la fraude ?
PE5 : La gestion des risques a un rôle essentiellement préventif. L'audit interne est plus centré sur la détection. Quant à l'audit externe, il intervient davantage dans la phase corrective : il détecte certains signaux et formule des recommandations, notamment sur l'efficacité du contrôle interne lié à la prévention de la fraude.
AZ: Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ?
PE5 : Non, pas vraiment. La distinction est généralement claire. Cependant, pour les clients ayant un contexte américain, l'auditeur externe joue un rôle plus approfondi dans l'évaluation du contrôle interne, ce qui peut créer un léger chevauchement avec l'audit interne. Mais au Luxembourg, la séparation des rôles reste bien définie.
AZ : Connaissez-vous les exigences de la norme ISA 240 ? Comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
PE5 : Oui. Selon la norme ISA 240, la responsabilité de l'auditeur externe consiste à s'assurer qu'un dispositif de prévention et de détection de la fraude est en place. L'auditeur ne cherche pas activement les cas de fraude comme le ferait un expert en forensic, mais il doit faire preuve de scepticisme professionnel et signaler toute indication de fraude aux autorités compétentes. Par exemple, au Luxembourg, cela se fait via la cellule responsable de la fraude ou la CSSF, selon la supervision de la société. En revanche, il ne faut pas informer le management, car celui-ci peut parfois être impliqué dans la fraude.
AZ : Quels outils ou techniques utilisez-vous pour identifier ou détecter des risques de fraude ?
PE5: Notre principal outil reste notre scepticisme professionnel, que l'on développe avec l'expérience. Ensuite, nous utilisons le test des écritures comptables (journal entry testing), qui consiste à analyser toutes les écritures de l'année pour détecter d'éventuelles anomalies. Cela reste toutefois limité aux aspects comptables et financiers ; les fraudes externes ou liées à des détournements physiques ne sont pas couvertes par cet outil.

AZ: Selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer la collaboration entre audit interne, audit externe et gestion des risques, ou aider à la détection de la fraude ?
PE5 : L'intelligence artificielle pourrait permettre des analyses de données plus poussées, notamment via le machine learning, pour identifier des tendances ou des anomalies. Cela serait particulièrement pertinent pour des organisations avec un grand volume de transactions, comme les banques ou les fonds d'investissement. Cependant, dans mon expérience, les analyses de l'audit interne reposent davantage sur des entretiens et des procédures que sur des données quantitatives, ce qui limite l'usage de l'IA pour certaines missions.
AZ: Pensez-vous que l'auditeur externe pourrait être davantage intégré dans la lutte contre la fraude ?
PE5 : Je ne pense pas. L'auditeur externe se base principalement sur les informations fournies par le management et sur les données financières disponibles. Son rôle reste limité à l'identification d'indicateurs de risque. Les auditeurs n'ont pas d'autorité pour enquêter ni pour sanctionner, et les dirigeants ne sont pas toujours obligés de tout divulguer. Le rôle de l'auditeur restera donc cantonné à l'évaluation du contrôle interne et à la formulation de recommandations.

Annexe 8 : Entretien 6 : Réviseur d'entreprise (Mandats Audit Interne), Code : PF6

AZ : Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
PF6: Je suis l'administrateur dirigeant et suis responsable de la gestion des services à nos clients.
AZ: Depuis combien d'années travaillez-vous dans ce domaine ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
PF6: J'ai ce rôle depuis 5 ans.
AZ: Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenu ?
PF6: Il n'y a eu aucune fraude financière (détournement d'argent) en interne. Par contre, un client a réalisé des opérations délictueuses par rapport à la loi (exportations non déclarées pour éviter les taxes) et nous avons l'obligation de le déclarer.
AZ: Comment définiriez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
PF6: Notre organisation est de petite taille et tout paiement est de mon ressort exclusif. De plus, un autre administrateur vérifie notre comptabilité régulièrement. Le principe des 4 yeux est donc respecté. Par le passé, dans une autre société, un employé avait fraudé (fausses notes de frais) et il a été licencié pour faute grave immédiatement.
AZ: Selon vous, quelles sont les responsabilités clés respectives de l'audit interne, de l'audit externe et de la gestion des risques dans ce domaine ?
PF6: L'audit externe peut détecter des montages de fraude (à la TVA par exemple) mais détectera rarement une fraude financière. L'audit interne a un rôle plus important en vérifiant les pouvoirs de signature sur les comptes bancaires et en analysant les comptes comptables impactés par les transactions financières. La gestion des risques permet d'avoir une vue globale sur les risques qu'encourt la Société, et notamment le risque de fraude.
AZ: Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ? Si oui, sur quels aspects ?
PF6: Les 3 fonctions ont un rôle dans la prévention et détection de la fraude. Les fonctions se complètent plutôt que se chevaucher.
AZ: La responsabilité en matière de détection de la fraude est-elle suffisamment claire dans votre organisation ? Pourquoi ?
PF6: Dans mon rôle d'administrateur, je suis responsable de toute fraude qui aurait lieu et aussi de mettre en place le contrôle interne défini pour limiter le risque de fraude.
AZ: Connaissez-vous les exigences de la norme ISA 240 ? Si oui, comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
PF6: Je confirme néanmoins que l'auditeur externe n'est pas responsable de détecter une fraude peu significative au regard des comptes annuels mais que si dans le cadre de son travail, il en identifie, il est responsable d'en informer la gouvernance de la société. Il convient de distinguer la fraude résultant de la mise en place de systèmes visant à tirer profit

d'une manœuvre avec but fiscal par exemple (c'est l'état qui est fraudé dans ce cas) et la fraude consistant à s'approprier des ressources de manière illégale (c'est la société elle-même ou un tiers qui est fraudé alors).
AZ: L'audit interne est-il, selon vous, positionné de manière stratégique pour jouer pleinement son rôle dans la lutte contre la fraude, tel que défini par les normes de l'IIA ?
PF6: L'audit interne est un rôle indépendant en relation directe avec la gouvernance. Il a pour but notamment de jouer un rôle de revue de la conformité des actes de la société par rapport aux règles et lois en vigueur. Dans ce cadre, il doit notamment analyser toute mise en place de flux ou processus afin d'en assurer la sécurité juridique et organisationnelle. Le défi de l'audit interne est de véritablement agir de manière indépendante et libre de la société.
AZ: Des divergences d'interprétation sur la mission de l'auditeur externe dans la détection de la fraude nuisent-elles, selon vous, à la collaboration interfonctionnelle ?
PF6: Oui, cela peut nuire dès lors qu'un rôle n'est pas clairement défini et communiqué. Il appartient à la gouvernance de la société de veiller à ce que les rôles soient bien définis et contribuent à couvrir tous les risques de fraude.
AZ: À quelle fréquence travaillez-vous en coordination avec les autres fonctions de contrôle (audit interne, gestion des risques, audit externe) ?
PF6: Il n'y a pas d'audit interne dans la société. La revue indépendante par un autre associé constitue le principal outil d'audit interne.
AZ: Existe-t-il dans votre organisation des dispositifs formels de coordination entre les fonctions (ex. : comités, plans d'audit concertés, réunions croisées) ?
PF6: Non, au vu de la taille de la société.
AZ: Quels outils ou techniques utilisez-vous pour identifier, évaluer ou détecter des risques de fraude ?
PF6: La revue continue des mouvements bancaires est appropriée dans les circonstances.
AZ: Partagez-vous ces résultats ou données avec d'autres fonctions de contrôle ? Si oui, par quels canaux ?
PF6: D'autres associés ont accès aux mouvements bancaires et peuvent donc identifier toute transaction suspecte.
AZ: Existe-t-il des processus formalisés de partage de l'information liée à la fraude entre audit interne, audit externe et gestion des risques ?
PF6: Rien de formalisé.
AZ: Observez-vous un risque de redondance ou de duplication dans les efforts de détection ou d'audit ? Si oui, comment cela pourrait-il être évité ?
PF6: Non, au vu de la taille de la société.
AZ: Votre organisation utilise-t-elle des outils de data analytics ou d'IA pour détecter des comportements frauduleux ?
PF6: Nous n'avons jamais fait face à une telle situation.
AZ: Selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer la collaboration entre audit interne, audit externe et gestion des risques ?

PF6: L'IA est dotée de capacité d'analyse sans limite et est une valeur ajoutée dans l'audit externe et interne.
AZ: Quelles sont les principales limites à l'adoption de ces technologies dans votre domaine (coût, formation, manque de stratégie, etc.) ?
PF6: Nous sommes abonnés à ChatGPT et utilisons cette technologie dans notre activité. Elle permet par exemple de vérifier la conformité par rapport à la loi de manière rapide et efficace. Elle peut aussi analyser une base de données de manière quasi instantanée.
AZ: Connaissez-vous des exemples de bonnes pratiques ou de modèles de collaboration réussie dans la lutte contre la fraude ?
PF6: Le principe des 4 yeux et la séparation des fonctions sont deux principes de base à respecter dans toute organisation qui se veut active contre le risque de fraude.
AZ: Si vous deviez formuler une recommandation pour améliorer la collaboration interfonctionnelle, quelle serait-elle ?
PF6: Conserver en tête les risques de fraude lorsqu'on met en place une procédure ou un rôle dans une organisation.
AZ: Selon vous, quel rôle la culture organisationnelle joue-t-elle dans la réussite (ou l'échec) d'une stratégie antifraude intégrée ?
PF6 : Nos collaborateurs sont formés au risque de fraude et aux moyens de le limiter. Cet élément de culture organisationnelle est essentiel pour lutter contre la fraude.

Annexe 9 : Entretien 7 : Partner, Business Risk Services (Audit Interne), Code : PG7

AZ : Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
PG7 : Associé (Partner) du département 'Business Risk Services' - actif dans les domaines de l'audit interne, contrôle interne et travaux réglementaires.
AZ : Depuis combien d'années travaillez-vous dans ce domaine ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
PG7 : 11 ans - uniquement en audit interne (audit interne dispensé en sous-traitance par notre cabinet pour les clients du secteur financier).
AZ : Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenu ?
PG7 : « Mon » organisation dans ce cas est Grant Thornton => non, aucune fraude. Dans le cadre de nos missions auprès de clients, nous avons été informés en 2019 par le Compliance officer de l'époque d'une fraude interne. Nous prestions la fonction d'audit interne à l'époque. Notre rôle (comme sous-traitant pour l'audit interne) a été relativement limité : le client et le compliance officer ont été très rapidement interrogés par les autorités de supervision (CSSF) qui sont montées au créneau, et ont par la suite retiré la licence d'établissement de l'entité en question. Nous avions démissionné de notre mandat d'audit interne pratiquement en même temps.
AZ : Comment définiriez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
PG7 : 1. Le rôle de la fonction d'audit interne vis-à-vis de la fraude est clairement énoncé dans les standards de la profession, et ne consiste pas en de la recherche/détection de fraude (cf. standard 4.2 Due Professional Care). 2. Prévention : nos travaux sont réalisés de manière à évaluer de manière générale l'exposition au risque de fraude et pouvoir produire des recommandations le cas échéant. 3. Gestion de la fraude : la gestion d'une fraude (enquête interne, etc.) peut faire partie des travaux d'un audit interne mais l'auditeur doit maîtriser les techniques d'investigations adaptées et appropriées au cas. Si l'auditeur ne dispose pas des compétences, il doit s'abstenir de mener le travail.
AZ : Selon vous, quelles sont les responsabilités clés respectives de l'audit interne, de l'audit externe et de la gestion des risques dans ce domaine ?
PG7 : Audit interne : cf. ci-dessus. Audit externe : l'auditeur externe a un rôle de détection de fraude possible en lien avec les états financiers, pour autant que les montants financiers soient au-dessus d'un seuil de matérialité défini par l'auditeur (c.-à-d. en dessous de ce seuil, toute incohérence de chiffres peut ne pas être expliquée). Gestion des risques : la fonction de gestion des risques est responsable d'une variété de typologies de risques selon l'environnement (financier, opérationnel, humain, légal, environnemental, etc.). Il est plutôt rare que la fonction de gestion des risques dispose dans ses attributions la lutte contre la fraude.
AZ : Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ? Si oui, sur quels aspects ?

PG7 : Oui, la perception que c'est la responsabilité de l'auditeur de détecter et trouver des fraudes est encore trop grande. Les gens ne comprennent pas bien le rôle de l'auditeur, et que ce dernier doit donner une assurance raisonnable, mais pas absolue, sur le degré de maîtrise des opérations de l'entité. La difficulté se trouve dans l'application du principe de « due professional care » et jusqu'où l'auditeur doit mener ses travaux et investigations pour atteindre ce niveau d'assurance « raisonnable ».
AZ : Connaissez-vous les exigences de la norme ISA 240 ? Si oui, comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
PG7 : Non.
AZ : L'audit interne est-il, selon vous, positionné de manière stratégique pour jouer pleinement son rôle dans la lutte contre la fraude, tel que défini par les normes de l'IIA ?
PG7 : Oui, cf. explications ci-dessus. L'auditeur interne peut être un atout dans la lutte / prévention de la fraude s'il est utilisé correctement et qu'on comprend bien son rôle d'assurance raisonnable et de conseiller.
AZ : Des divergences d'interprétation sur la mission de l'auditeur externe dans la détection de la fraude nuisent-elles, selon vous, à la collaboration interfonctionnelle ?
PG7 : Bien que les normes définissent la théorie à suivre, mon expérience me fait dire que la difficulté réside dans les besoins de communication/coordination entre les fonctions clés (2e ligne : compliance et gestion des risques) et l'audit externe. On parle ici d'« integrated assurance » – où les divers acteurs devraient se parler et se coordonner mieux. Aujourd'hui, pour les petites structures qui sous-traitent des travaux à l'extérieur, chacun regarde son périmètre sans trop se soucier de ce que les autres font. Cela amène des inefficacités et des duplications de travail et/ou des trous dans la couverture des fonctions clés.
AZ : À quelle fréquence travaillez-vous en coordination avec les autres fonctions de contrôle (audit interne, gestion des risques, audit externe) ?
PG7 : Cf. ci-dessus. Pour ce qui nous concerne (audit interne sous-traité pour des clients du secteur financier), la coordination est pratiquement inexistante ou très limitée.
AZ : Existe-t-il dans votre organisation des dispositifs formels de coordination entre les fonctions (ex. : comités, plans d'audit concertés, réunions croisées) ?
PG7 : Non.
AZ : Quels sont, selon vous, les principaux freins à une collaboration efficace ?
PG7 : Modèle de sous-traitance pas bien adapté pour cela (petits budgets, et intervention de l'audit interne une fois par an et pas trop en continu).
AZ : Quels facteurs ou leviers facilitent une synergie réussie entre ces fonctions ?
PG7 : Un vrai audit interne, en interne, facilite cette communication et coordination pour atteindre l'« integrated assurance ».
AZ : Quels outils ou techniques utilisez-vous pour identifier, évaluer ou détecter des risques de fraude ?
PG7 : Internal control questionnaire + interviews de staff.
AZ : Partagez-vous ces résultats ou données avec d'autres fonctions de contrôle ? Si oui, par quels canaux ?

PG7 : Non par défaut. Si une situation nous amenait (l'audit interne) à détecter un risque de fraude important, nous le reporterions à la direction autorisée et au conseil d'administration.
AZ : Existe-t-il des processus formalisés de partage de l'information liée à la fraude entre audit interne, audit externe et gestion des risques ?
PG7 : Je pense que oui.
AZ : Observez-vous un risque de redondance ou de duplication dans les efforts de détection ou d'audit ? Si oui, comment cela pourrait-il être évité ?
PG7 : Oui.
AZ : Votre organisation utilise-t-elle des outils de data analytics ou d'IA pour détecter des comportements frauduleux ?
PG7 : Non.
AZ : Selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer la collaboration entre audit interne, audit externe et gestion des risques ?
PG7 : Une IA pourrait potentiellement soulever rapidement les trous dans la raquette en matière de couverture de chacune des fonctions de contrôles et repérer les zones non contrôlées. Ce serait particulièrement intéressant dans un environnement de contrôle large et complexe. Dans une petite structure non complexe, ceci est aisément réalisé par un humain.
AZ : Quelles sont les principales limites à l'adoption de ces technologies dans votre domaine (coût, formation, manque de stratégie, etc.) ?
PG7 : La nature de nos travaux : nous sommes auditeurs internes pour des sociétés du secteur financier, en sous-traitance. Ce sont nos outils qui sont utilisés pour beaucoup de sociétés qui disposent de petits budgets et ne sont pas intéressées par des outils ou technologies pour ces sujets.
AZ : Connaissez-vous des exemples de bonnes pratiques ou de modèles de collaboration réussie dans la lutte contre la fraude ?
PG7 : Integrated assurance : approche holistique de la gouvernance qui coordonne différentes fonctions d'assurance.
AZ : Selon vous, quel rôle la culture organisationnelle joue-t-elle dans la réussite (ou l'échec) d'une stratégie antifraude intégrée ?
PG7 : Extrêmement important : le board doit montrer un tone at the top adéquat et promouvoir une culture de conformité et de gestion saine des risques.

Annexe 10 : Entretien 8 : Manager Audit Interne, Code : PH8

AZ : Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
PH8 : Je travaille en tant qu'auditeur dans le domaine de l'audit externe au Luxembourg. Auparavant, j'ai occupé le poste d'auditeur interne au sein du Label Vie (Carrefour), où j'ai conduit différentes missions de contrôle interne et d'investigation. Mon rôle actuel consiste à planifier et exécuter des missions d'audit légal, superviser des équipes et assurer la revue des travaux d'audit.
AZ : Depuis combien d'années travaillez-vous dans ce domaine ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
PH8 : J'ai 5 ans d'expérience combinée dans l'audit interne et externe, couvrant différents secteurs : immobilier, distribution, services, et construction.
AZ : Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenu ?
PH8 : Oui, dans une de mes expériences précédentes en audit interne, j'ai participé à une mission de détection et d'investigation de fraude dans le processus de gestion des stocks et d'inventaires. L'objectif était d'identifier les failles de contrôle et les pratiques frauduleuses, et de proposer des recommandations correctives.
AZ : Comment définiriez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
PH8 : L'audit interne joue un rôle clé dans la prévention et la détection de la fraude. Son rôle n'est pas d'être un « détective », mais de s'assurer que les dispositifs de contrôle interne sont efficaces et adaptés pour réduire les risques de fraude. Il peut également intervenir en investigation lorsqu'un soupçon est confirmé.
AZ : Selon vous, quelles sont les responsabilités clés respectives de l'audit interne, de l'audit externe et de la gestion des risques dans ce domaine ?
PH8 : Audit interne : prévention, renforcement des contrôles, sensibilisation et investigations ciblées. Gestion des risques : identification et évaluation des risques de fraude, intégration dans la cartographie des risques, suivi des plans d'action. Audit externe : évaluation du risque d'anomalies significatives dues à la fraude dans les états financiers, mise en œuvre de procédures ISA 240.
AZ : Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ? Si oui, sur quels aspects ?
PH8 : Oui, il existe des zones de recoupement, notamment entre audit interne et gestion des risques en matière d'évaluation des contrôles et d'alerte précoce. Ce chevauchement peut être positif s'il est bien coordonné.
AZ : La responsabilité en matière de détection de la fraude est-elle suffisamment claire dans votre organisation ? Pourquoi ?
PH8 : Elle est partiellement définie. L'audit externe reste focalisé sur les anomalies significatives, tandis que l'audit interne et la gestion des risques jouent un rôle plus

opérationnel. Une meilleure formalisation de la coordination permettrait de renforcer l'efficacité globale.
AZ : Connaissez-vous les exigences de la norme ISA 240 ? Si oui, comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
PH8 : Oui, la norme ISA 240 définit les responsabilités de l'auditeur externe pour identifier et évaluer les risques d'anomalies significatives résultant de fraudes et pour concevoir des procédures d'audit appropriées.
AZ : L'audit interne est-il, selon vous, positionné de manière stratégique pour jouer pleinement son rôle dans la lutte contre la fraude, tel que défini par les normes de l'IIA ?
PH8 : Oui, s'il est indépendant, bien structuré et intégré dans la gouvernance. L'audit interne dispose d'une connaissance approfondie des processus, ce qui lui permet d'identifier les vulnérabilités et d'alerter la direction.
AZ : Des divergences d'interprétation sur la mission de l'auditeur externe dans la détection de la fraude nuisent-elles, selon vous, à la collaboration interfonctionnelle ?
PH8 : Oui, certaines fonctions considèrent que la fraude relève essentiellement de l'audit interne, alors qu'elle devrait être abordée de manière transversale combinant audit interne, gestion des risques et audit externe.
AZ : À quelle fréquence travaillez-vous en coordination avec les autres fonctions de contrôle (audit interne, gestion des risques, audit externe) ?
PH8 : La coordination avait lieu de manière trimestrielle, avec des échanges ponctuels supplémentaires en cas d'alerte ou de suspicion de fraude.
AZ : Existe-t-il dans votre organisation des dispositifs formels de coordination entre les fonctions (ex. : comités, plans d'audit concertés, réunions croisées) ?
PH8 : Oui. Il existait des réunions périodiques avec la direction des risques et de la conformité, ainsi qu'un calendrier d'audit validé au niveau du comité interne. Ce dispositif permettait d'aligner les priorités de contrôle et d'éviter les doublons.
AZ : Comment qualifieriez-vous la qualité actuelle de la collaboration entre ces trois fonctions dans votre organisation (ou dans les organisations que vous connaissez) ?
PH8 : La collaboration était correcte mais pouvait être améliorée. Chacun avait une vision claire de ses responsabilités, mais les échanges restaient parfois réactifs plutôt que proactifs, surtout en dehors des périodes critiques.
AZ : Quels sont, selon vous, les principaux freins à une collaboration efficace ?
PH8 : Manque de communication continue, organisation en silos, confidentialité de certaines informations sensibles, absence de protocoles clairs pour le partage d'information.
AZ : Quels facteurs ou leviers facilitent une synergie réussie entre ces fonctions ?
PH8 : Des réunions de coordination régulières, des plans d'audit et cartographies de risques partagés, une culture de transparence, un rôle clair attribué à chaque fonction dès le lancement des missions.
AZ : Quels outils ou techniques utilisez-vous pour identifier, évaluer ou détecter des risques de fraude ?

PH8 : Tests analytiques ciblés, vérification physique des stocks, rapprochements de données, entretiens de contrôle, observation directe des opérations, revue des journaux de mouvements et vérification de la séparation des tâches.
AZ : Partagez-vous ces résultats ou données avec d'autres fonctions de contrôle ? Si oui, par quels canaux ?
PH8 : Oui. Les résultats étaient partagés principalement via les rapports d'audit, des réunions de clôture et des échanges formels avec la direction des risques et la direction générale.
AZ : Existe-t-il des processus formalisés de partage de l'information liée à la fraude entre audit interne, audit externe et gestion des risques ?
PH8 : Oui, mais partiellement. L'escalade des cas sensibles passait par une procédure interne documentée, mais le partage systématique entre toutes les fonctions n'était pas toujours automatisé.
AZ : Observez-vous un risque de redondance ou de duplication dans les efforts de détection ou d'audit ? Si oui, comment cela pourrait-il être évité ?
PH8 : Oui, notamment quand plusieurs services effectuent des contrôles similaires. Cela peut être évité grâce à une meilleure planification conjointe, une clarification des rôles et un calendrier partagé.
AZ : Votre organisation utilise-t-elle des outils de data analytics ou d'IA pour détecter des comportements frauduleux ?
PH8 : L'IA n'était pas encore utilisée, mais des analyses de données étaient effectuées via Excel ou Power BI et des outils internes pour détecter les anomalies.
AZ : Selon vous, en quoi l'intelligence artificielle pourrait-elle améliorer la collaboration entre audit interne, audit externe et gestion des risques ?
PH8 : Elle pourrait faciliter la centralisation des signaux faibles, automatiser la détection d'anomalies et permettre une priorisation plus rapide et objective des cas à investiguer. Cela favoriserait un langage commun entre les fonctions.
AZ : Quelles sont les principales limites à l'adoption de ces technologies dans votre domaine (coût, formation, manque de stratégie, etc.) ?
PH8 : Les principales limites sont le coût, le manque de formation du personnel, l'intégration avec les systèmes existants et l'absence d'une stratégie globale de lutte contre la fraude.
AZ : Connaissez-vous des exemples de bonnes pratiques ou de modèles de collaboration réussie dans la lutte contre la fraude ?
PH8 : Oui. Les collaborations les plus efficaces étaient celles où une cellule fraude réunissait audit interne, contrôle interne et risques pour examiner les alertes et coordonner les actions correctives.
AZ : Si vous deviez formuler une recommandation pour améliorer la collaboration interfonctionnelle, quelle serait-elle ?
PH8 : Instaurer une gouvernance claire avec une cellule commune antifraude, des réunions périodiques et une charte précisant les rôles et responsabilités de chaque acteur.

AZ : Selon vous, quel rôle la culture organisationnelle joue-t-elle dans la réussite (ou l'échec) d'une stratégie antifraude intégrée ?
PH8 : Un rôle essentiel. Une culture de transparence et de tolérance zéro à la fraude favorise les signalements et la coopération entre fonctions. À l'inverse, une culture de méfiance ou de silence complique la coordination et retarde la détection.

Annexe 11 : Entretien 9 : Directrice CPRO, Code : PI9

AZ : Pouvez-vous décrire brièvement votre poste actuel et vos responsabilités principales ?
PI9: Je dirige le pôle Contrôle Permanent et Risques Opérationnels .Je pilote le dispositif de contrôle, l'animation de la supervision managériale, la consolidation des incidents. Je coordonne aussi la cellule fraude avec les métiers, la Conformité et l'Inspection.
AZ: Depuis combien d'années travaillez-vous dans ce domaine ? Avez-vous occupé différents rôles dans la chaîne de contrôle ?
PI9: 13 ans dans la gestion des risques et le contrôle interne : analyste RO, puis responsable contrôle permanent, avant de prendre la direction CPRO
AZ: Votre organisation a-t-elle été confrontée à des cas de fraude au cours des cinq dernières années ? Si oui, dans quel cadre êtes-vous intervenue ?
PI9: Oui, des cas internes et externes (notamment tentatives de phishing et détournements). Le CPRO a coordonné l'évaluation, l'alerte aux instances, les mesures de remédiation et le suivi des plans d'actions et la cellule inspection a mené les investigations mais confidentielles.
AZ: Comment définiriez-vous la mission spécifique de votre fonction dans la prévention, la détection ou la gestion de la fraude ?
PI9: c'est le corps de notre métier en faite c'est prévenir par la cartographie et les contrôles, détecter via les indicateurs et outils de monitoring, et piloter la réponse opérationnelle (plans d'actions, risk acceptance) avec les métiers. Nous sommes l'« intégrateur » du dispositif anti-fraude.
AZ: Selon vous, quelles sont les responsabilités clés respectives de l'audit interne, de l'audit externe et de la gestion des risques dans ce domaine ?
PI9: CPRO/gestion des risques on est là pricipalement pour la prévention, pilotage du contrôle permanent et suivi des incidents.l'audit interne sont plus pour l'assurance indépendante et investigations.
AZ: Avez-vous le sentiment qu'il existe un chevauchement ou une confusion des rôles entre ces fonctions ? Si oui, sur quels aspects ?
PI9: Non les roles sont très bien définis au seins de la banque avec une separation des taches très claire.
AZ: La responsabilité en matière de détection de la fraude est-elle suffisamment claire dans votre organisation ? Pourquoi ?
Directrice : Oui : détection courante par les lignes de métiers via contrôles et KRIs ; investigation par Inspection ; reporting réglementaire par Conformité. On a des matrice qui formalisenn ces rôles.
AZ: Connaissez-vous les exigences de la norme ISA 240 ? Si oui, comment la responsabilité de l'auditeur externe face à la fraude y est-elle définie selon vous ?
PI9: Non pas spécifiquement.
AZ: L'audit interne est-il positionné de manière stratégique pour jouer pleinement son rôle (normes IIA) ?

PI9: Oui. Inspection couvre les processus clés, vérifie l'efficacité du contrôle permanent et suit les recommandations en comité. Son indépendance et l'accès libre à l'information sont garantis.
AZ: À quelle fréquence travaillez-vous en coordination avec les autres fonctions de contrôle ?
PI9: de façon journalière ou Hebdomadaire avec Conformité et inspection, mensuelle en comité fraude, et trimestrielle en comités de gouvernance.
AZ: Existe-t-il dans votre organisation des dispositifs formels de coordination entre les fonctions ?
PI9: Oui : comités fraude, plans de contrôle concertés et les cellule de crises.
AZ: Quels outils ou techniques utilisez-vous pour identifier, évaluer ou détecter des risques de fraude ?
PI9: cartographie dédiée fraude, KRIs, analyses d'incidents, scénarios, séparation des tâches, revues d'habilitations, suivi des comptes sensibles, centralisation des alertes (réclamations, SI, métier).
AZ: Partagez-vous ces résultats avec d'autres fonctions de contrôle ? Si oui, par quels canaux ?
PI9: Oui : tableaux de bord trimestriels, flash reports, comités, et workflow outillé pour l'escalade des incidents et le suivi des plans d'actions.
AZ: Votre organisation utilise-t-elle des outils de data analytics ou d'IA pour détecter des comportements frauduleux ?
PI9: Oui pour des règles de détection et des KRIs, l'IA est en pilote pour l'analyse de signaux faibles. Le déploiement complet dépend de la qualité des données et de la gouvernance des modèles.
AZ: Si vous deviez formuler une recommandation pour améliorer la collaboration interfonctionnelle, quelle serait-elle ?
PI9: je dirais avoir un référentiel commun des contrôles et incidents relié à un outillage partagé avec des KRI homogènes et une gouvernance claire des données.

8 Bibliographie

Al-Dhubaibi, A. A. S., & Sharaf-Addin, H. H. H. (2022). An analysis of external and internal auditors' use of ISA 240 red flags: The impact of auditors' estimation of fraud pervasiveness. Cogent Business & Management, 9(1), 2118209.

Association of Certified Fraud Examiners (ACFE). (2024). Occupational fraud 2024: A report to the nations. Austin, TX: Association of Certified Fraud Examiners.

Austin, A. A. (2023). Remembering fraud in the future: Investigating and improving auditors' attention to fraud during audit testing. Contemporary Accounting Research, 40(3), 925-951.

Bonrath, A., & Eulerich, M. (2023). Internal auditing's role in preventing and detecting fraud: An empirical analysis. International Journal of Auditing, 28(4), 615-631.

Carassus, D., & Cormier, D. (2003). Normes et pratiques de l'audit externe légal en matière de prévention et de détection de la fraude. Revue Française de Comptabilité, (345), 35–47.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise risk management: Integrating with strategy and performance. Durham, NC: American Institute of Certified Public Accountants (AICPA)

Demirović, L., Isaković-Kaplan, Š., & Proho, M. (2021). Internal audit risk assessment in the function of fraud detection. Journal of Forensic Accounting Profession, 1(1), 35–47.

DeZoort, F. T., & Harrison, P. D. (2016). Understanding Auditors' Sense of Responsibility for Detecting Fraud Within Organizations. Journal Of Business Ethics, 149(4), 857-874.

Drogalas, G., Pazarskis, M., Anagnostopoulou, E., & Papachristou, A. (2017). The effect of internal audit effectiveness, auditor responsibility and training in fraud detection. Accounting and Management Information Systems, 16(4), 434–454.

International Auditing and Assurance Standards Board (IAASB). (2009). Norme internationale d'audit (ISA) 240 : Les obligations de l'auditeur en matière de fraude lors d'un audit d'états financiers (traduction française par l'Institut des Réviseurs d'Entreprises [IRE] de Belgique et la Compagnie Nationale des Commissaires aux Comptes [CNCC]). In Handbook of International Standards on Auditing and Quality Control, 2009 Edition (ISBN 978-1-934779-92-7). International Federation of Accountants (IFAC).

International Auditing and Assurance Standards Board (IAASB). (2022). Norme internationale d'audit (ISA) 240 : Les obligations de l'auditeur en matière de fraude lors d'un audit d'états financiers (traduction française par l'Institut des Réviseurs d'Entreprises [IRE], la Compagnie Nationale des Commissaires aux Comptes [CNCC], et le Conseil supérieur de l'Ordre des Experts-Comptables [CSOEC]). In Handbook of International Quality Management, Auditing,

Review, Other Assurance, and Related Services Pronouncements, 2022 Edition, Volume I (ISBN 978-1-60815-546-0). International Federation of Accountants (IFAC).

Jizi, M., Nehme, R., & Elhout, R. (2017). Fraud: auditors' responsibility or organisational culture. International Social Science Journal, 66(4), 241-255.

Mangala, D., & Kumari, P. (2017). Auditors' perceptions of the effectiveness of fraud prevention and detection methods. Indian Journal of Corporate Governance, 10(2), 118–142

OpenAI. (2023). ChatGPT : reformulation, traduction, correction.

Petrașcu, D., & Tieanu, A. (2014, May 16–17). The role of internal audit in fraud prevention and detection. In 21st International Economic Conference 2014 (IECS 2014), Sibiu, Romania.

Simon, C. A., Smith, J. L., & Zimbelman, M. F. (2018). The influence of judgment decomposition on auditors' fraud risk assessments: Some trade-offs. The Accounting Review, 93(5), 273-291.

Simon, C. A., Smith, J. L., & Zimbelman, M. F. (2022). How fraud risk decomposition affects auditors' fraud risk assessments. Current Issues in Auditing, 16(1), P1–P9.

The Institute of Internal Auditors (IIA). (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense. Lake Mary, FL: The Institute of Internal Auditors.

The Institute of Internal Auditors (IIA). (2024). Normes internationales d'audit interne. Lake Mary, FL : The Institute of Internal Auditors.

Tilleman, B. (Dir.), Balestra, C., Dupont, L., Thirion, N., Tilleman, B., & Van Dyck, S. (2003). La responsabilité civile, pénale et disciplinaire du réviseur d'entreprises. Bruxelles : Institut des Réviseurs d'Entreprises / La Charte. ISBN 2-87403-089-9.

Verwey, I. G. F., & Asare, S. K. (2021). The joint effect of ethical idealism and trait skepticism on auditors' fraud detection. Journal of Business Ethics, 173(1), 149–171.

Wahidahwati, W., & Asyik, N. F. (2022). Determinants of auditors' ability in fraud detection. Cogent Business & Management, 9(1), 2130165.

Wang, I. Z., & Fargher, N. (2017). The effects of tone at the top and coordination with external auditors on internal auditors' fraud risk assessments. Accounting & Finance, 57(4),