الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

Mémoire de fin d'études

Spécialité : Management financier des entreprises

Le rôle du contrôle interne dans la prévention et la détection de la fraude

Etude de cas- Cas de fraude réel au seins d'une entreprise d'assurancde.

Présenté par :

IHADJADENE Silina Samia

Encadré par :

Dr. BOUCHETARA Mehdi

Année Universitaire : 2024/2025

Résumé

Ce mémoire a pour objectif d'analyser le rôle du contrôle interne dans la prévention et la détection de la fraude, à travers l'étude d'un cas réel survenu dans une entreprise d'assurance. La méthodologie adoptée repose sur une approche qualitative, mobilisant une étude de cas enrichie par des entretiens semi-directifs menés auprès de six cadres occupant des fonctions clés (direction, production, audit, finance, systèmes d'information). Les résultats montrent que la fraude a été rendue possible par des défaillances dans la séparatio des tâches, le suivi des anomalies et le contrôle hiérarchique. L'analyse met également en évidence le rôle central de la culture éthique, de la formation et des outils numériques dans le renforcement de l'efficacité du dispositif de contrôle interne. En conclusion, un contrôle interne bien conçu permet de limiter les risques de fraude, à condition qu'il soit soutenu par un engagement humain et organisationnel fort.

Key words : Internal control, Fraud prevention, Fraud detection, Corporate governance, Internal audit

Abstract

This research explores the role of internal control in preventing and detecting fraud within an insurance company, using a real-life case as the core of the analysis. A qualitative methodology was adopted, combining a case study approach with semi-structured interviews conducted with six managers from various hierarchical levels, including agency, regional, and central departments. The findings highlight significant weaknesses in task segregation, anomaly tracking, and managerial supervision that enabled fraudulent activities. The study also emphasizes the importance of ethical culture, employee training, and technological tools in enhancing internal control systems. Ultimately, the research concludes that while a well-structured internal control system is critical in mitigating fraud risks, its effectiveness depends heavily on human commitment and organizational vigilance.

Mots-clés : Contrôle interne, Prévention de la fraude, Détection de la fraude, Gouvernance d'entreprise, Audit interne

الملخص

يُسلِّط هذا البحث الضوء على دور نظام الرقابة الداخلية في الكشف عن الغش والحدّ منه داخل مؤسسة تأمين جزائرية، بالاعتماد على دراسة حالة حقيقية تم فيها توثيق عملية احتيال داخلية. تم اتباع منهجية نوعية قائمة على المقابلات شبه الموجهة مع مجموعة من الإطارات على مستويات تنظيمية متعددة، شملت الوكالة، الإدارة الجهوية، والإدارة المركزية. كشفت النتائج عن وجود ثغرات في منظومة الرقابة، خاصة فيما يتعلق بفصل المهام، ومتابعة العمليات غير النظامية، وضعف الرقابة الإدارية. كما أبرزت الدراسة أهمية ترسيخ ثقافة مؤسسية قائمة على الأخلاقيات، وتوفير تكوين مستمر في مجال مكافحة الغش، إلى جانب توظيف أدوات التحليل الرقمي لتعزيز فعالية الرقابة. وخلصت الدراسة إلى أن نجاح نظام الرقابة الداخلية لا يرتبط فقط بالإجراءات المطبقة، بل يتوقف على درجة التفاعل والالتزام من طرف الأفراد والهيئات الرقابية داخل المؤسسة

ِالكلمات المفتاحية

الرقابة الداخلية، الوقاية من الاحتيال، كشف الاحتيال، حوكمة الشركات، التدقيق الداخلي

Remerciements

La réalisation de ce mémoire de fin d'études représente l'aboutissement d'un parcours académique riche en apprentissages et en défis. Ce travail n'aurait pu voir le jour sans le soutien, l'encadrement et la bienveillance de nombreuses personnes, que je tiens à remercier ici avec la plus grande reconnaissance.

Je tiens tout d'abord à adresser mes remerciements les plus sincères à **Monsieur Bouchetara Mehdi**, mon encadrant universitaire, pour son accompagnement rigoureux, sa disponibilité constante et la qualité de ses conseils. Sa pédagogie exigeante et son sens du détail ont été des leviers essentiels dans la structuration et la réussite de ce travail. J'espère avoir répondu aux attentes qu'il incarne et honoré sa confiance.

Je remercie par ailleurs **le président du jury ainsi que l'ensemble des membres examinateurs** pour l'honneur qu'ils me font en évaluant ce travail. Veuillez trouver ici l'expression de ma plus haute considération.

Je souhaite également exprimer ma profonde gratitude à **mes parents**, pour leur amour inconditionnel, leur patience et les sacrifices qu'ils n'ont cessé de faire pour m'offrir les meilleures conditions de réussite. Leur présence discrète mais déterminante a été pour moi un pilier tout au long de mon parcours. À mon **frère** et à mes **sœurs**, je témoigne toute mon affection et ma reconnaissance pour leur soutien indéfectible, leur compréhension et leurs encouragements constants.

Je souhaite remercier chaleureusement **l'ensemble des membres de PwC** qui m'ont accueilli au sein de leur structure avec professionnalisme et bienveillance. Leur disponibilité, la richesse des échanges et la qualité de leur accompagnement ont contribué de manière significative à la portée pratique de ce mémoire.

Mes pensées reconnaissantes s'adressent également à **l'ensemble de mes enseignants**, pour la qualité de l'enseignement dispensé tout au long de mon cursus. Grâce à leur engagement et à la transmission généreuse de leur savoir, j'ai pu acquérir des compétences solides, tant académiques que professionnelles.

Enfin, je tiens à remercier du fond du cœur **mes amis**, pour leur présence fidèle, leur soutien moral, et leur amitié sincère.

À toutes les personnes qui, de près ou de loin, ont contribué à la réussite de ce travail, je dis avec humilité et sincérité : **merci**.

Liste des tableaux :

Liste des figures :

Liste des abréviatons,sigles et acronymes

- **ACFE** : Association of Certified Fraud Examiners
- **AI** : Intelligence Artificielle
- **AICPA** : American Institute of Certified Public Accountants
- **AMF** : Autorité des Marchés Financiers
- **BI** : Business Intelligence
- **CIA** : Certified Internal Auditor
- **CFE** : Certified Fraud Examiner
- **CISA** : Certified Information Systems Auditor
- **COBIT** : Control Objectives for Information and Related Technologies
- **COSO** : Committee of Sponsoring Organizations of the Treadway Commission
- **CPA** : Certified Public Accountant
- **CRM** : Customer Relationship Management
- **EBITDA** : Earnings Before Interest, Taxes, Depreciation and Amortization
- **ERP** : Enterprise Resource Planning
- **EY** : Ernst & Young
- **GAAP** : Generally Accepted Accounting Principles
- **GDPR / RGPD** : General Data Protection Regulation / Règlement Général sur la Protection des Données
- **GRC** : Governance, Risk, and Compliance
- **IAASB** : International Auditing and Assurance Standards Board
- **IAS / IASB** : International Accounting Standards / Board
- **IFAC** : International Federation of Accountants
- **IFACI** : Institut Français de l'Audit et du Contrôle Interne

- **IFRS** : International Financial Reporting Standards
- **IIA** : Institute of Internal Auditors
- **ISA** : International Standards on Auditing
- **ISO** : International Organization for Standardization
- **IT** : Information Technology
- **KPMG** : Klynveld Peat Marwick Goerdeler
- **ML** : Machine Learning
- **PCAOB** : Public Company Accounting Oversight Board
- **PwC** : PricewaterhouseCoopers
- **ROA / ROE** : Return on Assets / Return on Equity
- **ROI** : Return on Investment
- **RSE** : Responsabilité Sociétale des Entreprises
- **SAP** : Systems, Applications and Products in Data Processing
- **SEC** : Securities and Exchange Commission
- **SOX** : Sarbanes-Oxley Act
- **IARD** : Incendie, Accidents et Risques Divers

Sommaire

Sommaire

Introduction générale

Dans un environnement économique caractérisé par la montée des incertitudes, la pression concurrentielle et l'intensification des exigences réglementaires, la **fraude interne** apparaît comme une menace systémique pour les organisations, quel que soit leur secteur d'activité. Elle compromet non seulement la fiabilité de l'information financière, mais également la confiance des parties prenantes, la solidité des processus internes et la réputation de l'entreprise (Putra et al, 2022). Cette problématique est d'autant plus critique dans les secteurs régulés, tels que l'assurance, où les enjeux de transparence, de conformité et de gestion des risques sont particulièrement sensibles.

Face à ces défis, le **contrôle interne** s'impose comme un mécanisme essentiel de régulation et de gouvernance (Henk,2020). Bien au-delà de sa fonction historique de vérification comptable, il constitue aujourd'hui un **dispositif intégré de prévention, de détection et de maîtrise des risques (Roussy, and Perron, 2018)** , y compris ceux liés à la fraude. Le cadre normatif international, notamment le référentiel COSO et la norme ISO 31000, consacre le contrôle interne comme un pilier de la stratégie organisationnelle (Henk, 2020). Cependant, son efficacité dépend de multiples facteurs : conception des procédures, engagement managérial, culture de l'éthique, qualité des outils de supervision, entre autres (Rorie, and West, 2020).

Dès lors, la question centrale à laquelle ce mémoire tente de répondre est la suivante :
Dans quelle mesure le contrôle interne permet-il de prévenir et de détecter efficacement la fraude au sein des organisations, et comment son efficacité peut-elle être optimisée dans la pratique ?

Ce travail vise à apporter des éléments de réponse à travers une démarche scientifique articulant **cadre conceptuel rigoureux** et **étude de cas approfondie** d'une situation réelle de fraude dans une agence d'assurance. Cette double approche, à la fois théorique et empirique, permet de confronter les référentiels et bonnes pratiques aux réalités du terrain.

Ce mémoire présente un double intérêt. Sur le plan **académique**, il contribue à enrichir les travaux portant sur l'efficacité du contrôle interne dans la maîtrise des risques de fraude, en

mobilisant les modèles de référence (triangle de la fraude de Cressey, COSO, ISA 240, etc.) et en s'appuyant sur des études de cas documentées (Enron, Parmalat, Wirecard). Sur le plan **opérationnel**, il offre une lecture critique d'un dispositif réel, assortie de recommandations concrètes à destination des managers et auditeurs internes, en vue d'optimiser les mécanismes de prévention et de surveillance.

Comme tout travail empirique, cette recherche présente certaines **limites**. Elle repose sur une **étude de cas unique**, ce qui en limite la portée généralisable. Les données recueillies proviennent essentiellement d'**entretiens qualitatifs**, ce qui peut introduire des biais liés à la subjectivité des répondants ou à la sensibilité du sujet traité. De plus, pour des raisons de confidentialité, certains éléments ont été volontairement anonymisés.

La méthodologie adoptée s'inscrit dans une approche **qualitative interprétative**, fondée sur une étude de cas exploratoire. Les données ont été collectées à travers plusieurs canaux : entretiens semi-directifs avec des responsables de différents niveaux hiérarchiques (direction d'agence, direction régionale, directions centrales), observation des processus, et analyse documentaire (procédures internes, organigrammes, notes de service, normes professionnelles). Une **analyse thématique** a ensuite été menée afin d'identifier les points de rupture, les défaillances du contrôle et les leviers d'amélioration.

CHAPITRE 1 : cadre conceptuel du rôle du contrôle interne dans la prévention et la lutte contre la fraude

Chapitre 1 : cadre conceptuel du rôle du contrôle interne dans la prévention et la lutte contre la fraude :

Introduction :

Afin de bien comprendre l'importance du contrôle interne dans la lutte contre la fraude, il est essentiel d'explorer au préalable les concepts qui y sont associés. Ce premier chapitre aura pour objectif de poser les bases théoriques nécessaires à l'assimilation du rôle que le contrôle interne joue dans la prévention et la détection des comportements frauduleux. Il sera divisé en trois sections, chacune traitant d'une dimension spécifique du sujet.

Section 1 : La fraude interne

La fraude interne représente un des risques les plus importants pour les organisations. Elle peut prendre de nombreuses formes, allant du vol d'actifs physiques ou immatériels à la manipulation des informations financières. Elle implique généralement un ou plusieurs employés de l'organisation, et peut être motivée par des raisons financières, personnelles ou même organisationnelles.

Dans cette section, nous commencerons par définir ce qu'est la fraude interne, ses différentes formes (fraude comptable, manipulation des informations financières, corruption interne, etc.), et ses conséquences tant sur la santé de l'organisation que sur la confiance des parties prenantes. Cette analyse permettra de poser les bases nécessaires pour comprendre pourquoi il est crucial de mettre en place des systèmes de prévention et de détection efficaces.

Section 2 : Techniques de lutte contre la fraude

Une fois que la fraude interne est définie et que ses formes et ses risques sont compris, il devient essentiel d'explorer les techniques et mécanismes permettant de lutter contre elle. Ces techniques incluent à la fois des actions préventives et des dispositifs de détection.

Nous aborderons ici les différentes stratégies de prévention, telles que la formation des employés, l'instauration d'une culture organisationnelle éthique, ainsi que la mise en place de contrôles externes et internes. Ensuite, nous explorerons les outils et technologies qui permettent de détecter rapidement les fraudes, qu'il s'agisse de logiciels de détection

d'anomalies, de vérifications régulières des comptes, ou encore de mécanismes de dénonciation.

Cette section mettra en lumière les meilleures pratiques et stratégies qui, lorsqu'elles sont appliquées de manière rigoureuse, permettent de réduire considérablement le risque de fraude au sein de l'entreprise.

Section 3 : Le contrôle interne

Le contrôle interne, en tant que concept, constitue le cœur de la prévention et de la détection de la fraude. Il fait référence à l'ensemble des processus mis en place par une organisation afin de garantir la fiabilité de l'information financière, la conformité aux lois et régulations, ainsi que la protection des ressources de l'organisation contre toute forme de fraude ou d'erreur.

Dans cette dernière section, nous définirons le contrôle interne et ses objectifs principaux, tels que la prévention des erreurs et des fraudes, la mise en place d'une surveillance continue des activités de l'entreprise, et la réduction des risques liés aux erreurs humaines ou systèmes. Nous examinerons également les différents modèles de contrôle interne, comme celui du COSO (Committee of Sponsoring Organizations of the Treadway Commission), et comment ces modèles peuvent être appliqués pour garantir une gestion efficace de la fraude.

Nous verrons également les rôles clés des acteurs du contrôle interne, tels que le comité d'audit, les auditeurs internes, et les responsables des départements de conformité et de gestion des risques. Enfin, nous mettrons en lumière l'interaction entre le contrôle interne et la détection de la fraude, en expliquant comment un système de contrôle bien conçu peut permettre non seulement de prévenir les fraudes, mais aussi de les identifier rapidement.

Introduction :

Dans un contexte économique marqué par une complexité croissante et une multiplication des risques de toute nature, la fraude interne constitue une menace majeure pour les entreprises et les institutions. Face à cette problématique, la mise en place d'un cadre conceptuel solide s'impose, intégrant plusieurs notions clés : la fraude elle-même, les dispositifs de contrôle interne, la gestion des risques et les méthodes de prévention.

Le contrôle interne apparaît comme un levier fondamental dans la lutte contre la fraude. Il repose sur un ensemble de processus, de politiques et de procédures visant à assurer la fiabilité des opérations, la conformité aux réglementations et la protection des actifs de l'entreprise. Un contrôle interne efficace permet non seulement de détecter les irrégularités, mais surtout d'en prévenir l'apparition en réduisant les possibilités de fraude.

Dans cette optique, l'analyse des risques liés à la fraude revêt une importance capitale. Il s'agit d'identifier les vulnérabilités organisationnelles, ainsi que leur impact potentiel sur les activités de l'entreprise. Cette approche permet de concevoir des stratégies adaptées, combinant des mesures réglementaires, des outils de surveillance et une sensibilisation accrue des acteurs internes.

Ainsi, cette étude vise à explorer le rôle du contrôle interne en tant que dispositif central de prévention et de détection de la fraude, tout en mettant en lumière les interactions entre la gestion des risques et les stratégies de prévention et de contrôle interne permettant d'y faire face.

Section 1 : Concept et typologie de la fraude interne.

Dans ce travail, nous proposons d'explorer le cadre conceptuel de la fraude en intégrant plusieurs dimensions clés. Tout d'abord, nous définissons la fraude en tant que comportement intentionnel visant à tromper pour obtenir un avantage indu. Nous poursuivrons en présentant ses typologies établies selon divers critères—tels que l'origine (fraude interne vs externe), l'intention ou l'objectif recherché (enrichissement personnel et présentation trompeuse de l'entreprise), ainsi que la nature des méthodes utilisées (détournement d'actifs, manipulation comptable, etc.).

Nous introduisons ensuite le modèle du triangle de Cressey, qui identifie trois facteurs fondamentaux – pression, opportunité et rationalisation – comme des éléments déterminants dans la manifestation de comportements frauduleux. Pour illustrer concrètement ces concepts, nous analyserons enfin plusieurs cas réels de fraudes, parmi lesquels des scandales emblématiques tels que Enron, Parmalat ou Wirecard, afin de comprendre comment les mécanismes de fraude se déploient dans la pratique et quelles leçons peuvent être tirées pour renforcer les dispositifs de prévention et de détection.

Cette approche intégrée vise à fournir une vision globale du phénomène frauduleux, enrichissant notre compréhension des mécanismes internes et externes de la fraude, et soulignant l'importance d'une gouvernance rigoureuse dans un environnement économique complexe.

1.1 Définition de la fraude

La fraude est un concept transversal qui revêt diverses formes selon les contextes dans lesquels elle se manifeste. Elle peut être définie comme toute action volontaire et intentionnelle allant à l'encontre des principes d'intégrité et de transparence, qu'elle soit illégale ou simplement contraire à l'éthique. Cela inclut des pratiques telles que les pots-de-vin, la corruption ou encore les conflits d'intérêts, qui faussent la concurrence et érodent la confiance au sein des relations économiques et sociales.

La norme ISA 240, qui traite du rôle des auditeurs dans la détection de la fraude, définit celle-ci de manière implicite comme « un acte intentionnel commis par une ou plusieurs personnes au sein de l'entreprise – qu'il s'agisse de membres de la direction, de responsables de la gouvernance, d'employés ou de tiers – dans le but de tromper pour obtenir des avantages illégaux ou injustifiés ». Cette norme distingue deux types principaux de fraude : d'une part, celle liée à la manipulation des états financiers, et d'autre part, celle découlant du détournement d'actifs.(norme ISA 240, 2023)

Par ailleurs, la fraude s'inscrit dans une pluralité de dimensions éthiques, juridiques et institutionnelles. Selon l'Association of Certified Fraud Examiners (ACFE), elle se définit comme « l'exploitation abusive de son poste ou de ses responsabilités professionnelles afin de s'enrichir personnellement, notamment par le détournement ou l'usage illégal des ressources ou des actifs de l'entreprise ». En d'autres termes, elle consiste en l'abus d'une position interne

dans le but d'obtenir un gain financier illégitime au détriment de l'organisation.(Frédéric Bernard-Rémi Gayaraud-Laurent rousseau, 2008)

Enfin, dans le domaine de la cybersécurité, la fraude prend une dimension particulièrement préoccupante. Les avancées technologiques et la digitalisation croissante ont permis aux fraudeurs de développer des techniques sophistiquées, telles que l'hameçonnage (phishing), l'usurpation d'identité ou l'accès frauduleux à des systèmes d'information. Ces attaques exploitent les failles des dispositifs de sécurité pour voler des données sensibles, détourner des fonds ou saboter des opérations.(Mirinaviciene, 2014) Les normes de cybersécurité, telles que l'ISO 27001, mettent en avant l'importance de stratégies robustes de prévention, incluant la formation des utilisateurs, la surveillance des réseaux et le renforcement des systèmes de protection.

1.2 Classification des fraudes selon différents critères

Pour appréhender pleinement le phénomène frauduleux et orienter les stratégies de contrôle à adopter, il convient d'élaborer une classification reposant sur plusieurs axes. Dans le cadre de cette étude, nous examinerons la fraude selon trois critères majeurs : l'origine (ou l'auteur), l'intention (ou l'objectif) et la nature des méthodes employées. À cette analyse s'ajoute également l'intégration du modèle théorique du triangle de la fraude, qui éclaire les facteurs sous-jacents à ces comportements.

1.2.1 Classification par l'Auteur ou l'Origine

Notre première approche consiste à distinguer les fraudes en fonction de l'origine des acteurs impliqués. Ainsi, nous pouvons distinguer :

- La fraude interne : La fraude interne est commise par des individus travaillant au sein d'une organisation, tels que des employés, des cadres ou même des dirigeants. Selon les travaux de l'Association of Certified Fraud Examiners (ACFE), elle englobe des comportements tels que le détournement d'actifs, la falsification de documents internes, ou encore l'abus de position dans le but d'obtenir des gains personnels. Ziegenfuss (1996) identifie la fraude interne comme un défi éthique majeur, où l'accès privilégié aux ressources et aux processus facilite les actes frauduleux. Des exemples incluent le vol d'argent, la manipulation de comptes ou le transfert illégal de propriétés. Sa détection est souvent difficile car les auteurs connaissent bien les processus internes et peuvent profiter des failles de contrôle. D'après les statistiques mondiales de l'ACFE,

la fraude interne par détournement d'actifs est la plus fréquente (elle représente environ 89 % des cas étudiés) bien que généralement la moins coûteuse en montant médian – en revanche, les fraudes impliquant la manipulation des états financiers par les dirigeants, plus rares (5 % des cas), causent en moyenne les pertes les plus lourdes (plusieurs centaines de milliers de dollars par cas)(Mirinaviciene, 2014)

Ces actions nuisent gravement à la confiance interne et exigent une surveillance accrue ainsi que des contrôles rigoureux pour les prévenir.

- La fraude externe : La fraude externe, quant à elle, est perpétrée par des acteurs extérieurs à l'organisation : clients, fournisseurs, hackers, ou autres tiers. Green (2004) met en lumière l'ampleur de la cyberfraude, qui inclut des pratiques comme le phishing, les attaques de ransomware ou l'usurpation d'identité numérique. Ce type de fraude vise à exploiter les vulnérabilités des systèmes informatiques ou les failles contractuelles. En outre, des pratiques telles que les fausses déclarations ou la présentation frauduleuse de produits font également partie de cette catégorie. La prévention de la fraude externe requiert des solutions technologiques avancées, comme le renforcement des systèmes de cybersécurité et l'amélioration des protocoles de vérification.

Dans le cadre de notre étude, une attention particulière sera portée au rôle du contrôle interne dans la prévention et la détection de la fraude. Le contrôle interne constitue un pilier essentiel pour garantir l'intégrité des processus organisationnels. Par des mécanismes tels que la séparation des tâches, les vérifications régulières et l'utilisation d'outils de supervision, il vise à réduire les opportunités de fraude interne tout en renforçant la capacité des organisations à identifier et à répondre rapidement aux menaces externes. En nous concentrant sur cette dimension, nous chercherons à démontrer comment un système de contrôle interne robuste peut agir comme une première ligne de défense contre les comportements frauduleux.(Chekroun, 2017)

Classification par l'objectif ou l'intention

Bien qu'aucune fraude ne se fasse sans viser un avantage indu, il est néanmoins pertinent de distinguer, sur le plan de l'intention, deux grandes orientations(Rachid, 2022):

- L'enrichissement personnel direct :

Dans ce cadre, le fraudeur détourne financièrement des fonds ou des actifs (par exemple, en recourant à la création de fournisseurs fictifs, en effectuant des vols ou en percevant des pots-de-vin) dans le seul but d'obtenir un profit immédiat. Ce type d'infraction se traduit directement par un manque à gagner pour l'organisation.

- La manipulation stratégique au profit de l'entité :

Ici, la fraude vise à embellir artificiellement l'image financière de l'entreprise afin d'attirer des investisseurs ou de dissimuler des difficultés. Le scandale Enron, par exemple, illustre comment une manipulation des comptes, à l'aide notamment d'outils tels que l'utilisation de structures hors bilan, a permis de maintenir une valorisation attractive malgré des pertes considérables. Dans ce cas, les motivations peuvent être multiples, mêlant des intérêts personnels à une logique de survie de l'entreprise.

1.2.3 Classification par la Nature ou les Méthodes Employées :

Selon la taxonomie proposée par l'ACFE, souvent représentée sous la forme d'un « fraud tree », la fraude peut se diviser en trois grandes catégories, bien qu'il subsiste de nombreuses typologies spécifiques (comme la fraude à la facturation, à la paie, fiscale ou aux investissements)(Mirinaviciene, 2014, p. 173)

❖ Fraude sur les États Financiers (Financial Statement Fraud)

La fraude sur les états financiers désigne toute manipulation intentionnelle des rapports comptables afin de présenter une image trompeuse de la situation financière d'une entreprise. Cela peut inclure :

- **Manipulations comptables :** Les dirigeants ou les employés modifient délibérément les écritures comptables pour influencer les résultats financiers, par exemple en gonflant les chiffres de ventes ou en omettant des dettes importantes.
- **Falsification de documents :** Cela concerne la production ou l'altération de documents comptables, tels que des factures ou des relevés bancaires, pour dissimuler des activités frauduleuses ou falsifier des résultats.

Un exemple fréquent est celui d'un employé créant de fausses factures ou modifiant des écritures comptables pour détourner une partie des fonds de l'entreprise. Ce type de fraude peut survenir dans des départements de facturation où le contrôle interne est relativement faible.

- **Dissimulation des provisions ou passifs :** Il s'agit de sous-estimer les provisions pour pertes ou de cacher des dettes dans les rapports financiers afin de montrer une rentabilité artificiellement élevée.

- Utilisation de structures hors bilan (Off-balance-sheet entities) : Cette pratique consiste à créer des entités externes pour y transférer les dettes de l'entreprise, réduisant ainsi artificiellement son niveau d'endettement. Un cas célèbre est celui d'Enron, où des filiales fictives ont été utilisées pour camoufler des pertes massives et gonfler les bénéfices déclarés.

❖ Fraude Comptable au Sein des Entreprises :

Selon les normes internationales IFRS et les standards ISA240 en 2009, la fraude comptable inclut toutes les manipulations intentionnelles visant à présenter une image déformée des performances ou de la situation financière de l'organisation. Les pratiques typiques comprennent :

- **Falsification et modification des documents :** Cela inclut la création de faux documents, comme des factures ou des écritures fictives, pour dissimuler des transactions illégales ou détourner des fonds.
- **Surévaluation des revenus :** Il s'agit de comptabiliser des revenus non encore perçus ou de déclarer des ventes fictives, ce qui fausse les indicateurs financiers tels que le chiffre d'affaires et la rentabilité.
- **Minimisation des charges :** Les dépenses réelles de l'entreprise sont intentionnellement sous-évaluées afin de montrer une amélioration artificielle des marges bénéficiaires.
- **Manipulation des provisions :** Les entreprises ajustent leurs provisions pour pertes ou créances douteuses afin de masquer leurs difficultés financières.On peut citer comme exemple le secteur bancaire, il arrive que des établissements ne mettent pas à jour correctement leurs provisions pour créances douteuses, dissimulant ainsi le risque réel d'une détérioration de leur portefeuille de prêts. Ce réajustement artificiel permet d'afficher une performance plus favorable.
- **Pratiques frauduleuses d'audit interne :** Les informations fournies lors des audits sont volontairement incomplètes ou erronées, empêchant les régulateurs de détecter les irrégularités.

Un responsable de l'audit interne pourrait, par exemple, négliger volontairement de vérifier certaines transactions suspectes ou falsifier des rapports d'audit afin de cacher des irrégularités.

Cette omission délibérée compromet l'intégrité du processus de vérification et favorise la dissimulation d'actes frauduleux.

- **L'utilisation des structures hors bilan (Off-Balance-Sheet Entities) :** Les structures hors bilan représentent un mécanisme souvent employé dans le cadre de fraudes comptables. Elles consistent à créer des entités distinctes ou des sociétés-écrans pour y transférer des dettes, des passifs ou des actifs problématiques afin de réduire artificiellement le niveau d'endettement ou de gonfler les bénéfices déclarés de l'entreprise. Cette pratique, bien qu'acceptable dans certains cadres réglementaires spécifiques, est souvent détournée à des fins frauduleuses. Un exemple emblématique est celui de la faillite d'Enron en 2001, où l'entreprise a utilisé des entités hors bilan pour cacher des milliards de dollars de dettes et améliorer artificiellement ses résultats financiers, trompant ainsi les investisseurs et les régulateurs. Les risques associés à l'utilisation des structures hors bilan incluent la complexité accrue des états financiers – rendant difficile la détection des irrégularités – ainsi que l'opacité des transactions entre l'entreprise et ses filiales ou entités liées. Dans le cadre des audits, une vigilance particulière est requise pour s'assurer que ces structures respectent les principes comptables et ne dissimulent pas des manipulations frauduleuses.

L'utilisation des structures hors bilan illustre comment des mécanismes comptables complexes peuvent être exploités pour déformer la réalité financière, soulignant la nécessité d'audits rigoureux et de réglementations renforcées. Un exemple marquant est la faillite d'Enron en 2001, qui a révélé des pratiques massives de fraude comptable : des sociétés-écrans et des entités hors bilan ont été utilisées pour cacher des passifs et gonfler artificiellement les bénéfices. Cette affaire a mis en lumière l'importance de contrôles stricts et d'une supervision accrue pour éviter de tels scandales.

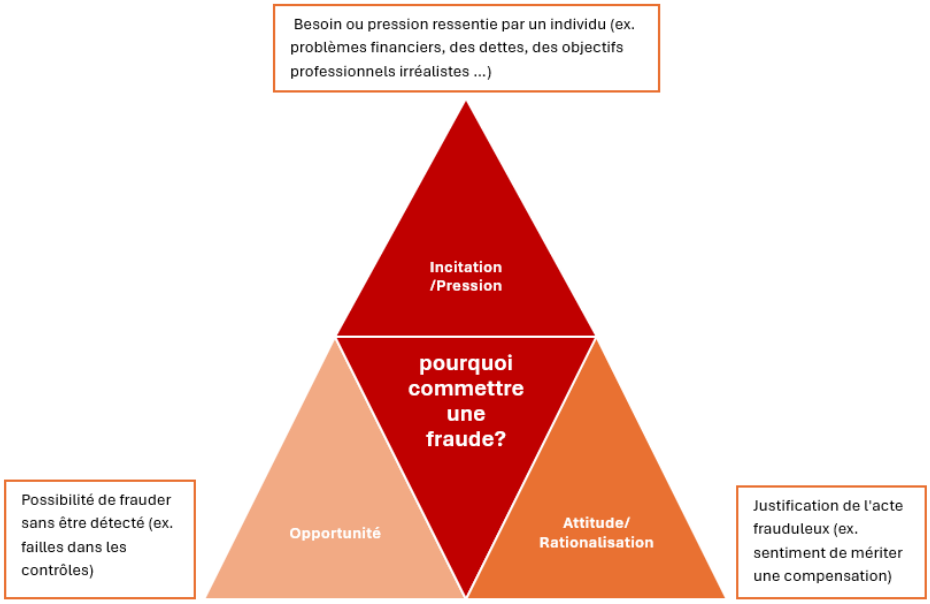
En conclusion, la classification des fraudes en interne et externe, ainsi que les différentes méthodes employées, permet de mieux comprendre les mécanismes de fraude. Cette compréhension est cruciale pour adapter les stratégies de contrôle interne et de prévention. Le modèle du triangle de Cressey, avec ses trois facteurs clés (pression, opportunité, rationalisation), offre une perspective utile pour analyser les comportements frauduleux.

1.4 Le triangle de la fraude *:*

Enfin, pour mieux comprendre les facteurs favorisant la fraude, il est essentiel d'appliquer le modèle du triangle de la fraude de Donald Cressey, qui identifie trois éléments clés interagissant pour créer un environnement propice à la fraude

Le triangle de la fraude est un concept élaboré par le criminologue Donald Cressey en 1950, il s'agit d'une tentative de théoriser de façon simple les différents aspects de la fraude d'un point de vue anthropologique. Ce concept aujourd'hui est utilisé dans la grande majorité des universités pour enseigner le concept de fraude, mais est aussi utilisé en audit chez les plus grands cabinets afin d'approcher le risque de fraude. Le triangle identifie trois facteurs clés qui expliquent pourquoi une personne peut commettre une fraude.

Figure 1 : Le triangle de Cressey



Source : document interne de PwC

Selon le schéma ci-dessus, identifie, donc, trois facteurs clés qui expliquent les raisons qui pourraient pousser une personne à commettre une fraude :

L'opportunité (Opportunity): se produit lorsque les contrôles internes sont insuffisants ou inefficaces. Une surveillance faible ou une absence de contrôle facilite la commission de fraudes. L'audit interne joue un rôle crucial en réduisant ces opportunités en améliorant les contrôles**.**

La pression (ou motivation) (Pressure)

Elle peut être financière, personnelle ou professionnelle : endettement, attentes de performance élevées, ou menaces de licenciement. Les employés sous pression sont plus susceptibles de justifier des actes frauduleux.

La rationalisation (Rationalization)

Justification morale de l'acte frauduleux exemple : « Je suis sous-payé, donc c'est normal de me compenser moi-même. »(Desai, 2020) Une culture éthique forte et des formations à l'intégrité peuvent limiter ce facteur

Le modéle de Cressey permet non seulement de comprendre la genèse des fraudes, mais aussi d'identifier les leviers d'intervention pour réduire ces risques—bien que les mesures de prévention et de détection soient détaillées dans le point ci-dessus.

1.3. Études de cas de fraudes réelles :

Afin d'illustrer concrètement les typologies et mécanismes de fraude présentés précédemment, nous examinerons trois cas emblématiques de fraude financière et comptable : ceux d'Enron, de Parmalat et de Wirecard. Ces affaires, qui se sont déroulées dans des contextes géographiques, sectoriels et temporels variés, offrent un éclairage approfondi sur la façon dont les fraudes ont été orchestrées, détectées et sur les conséquences économiques et réglementaires qu'elles ont engendrées. De plus, l'analyse de ces exemples contribue à comprendre comment ces scandales ont influencé et façonné les pratiques actuelles de régulation et de contrôle en matière de lutte contre la fraude.

1.3.1 Le scandale Enron (2001) – Fraude comptable interne au sommet de l'entreprise :

A. Contexte et importance du cas :

Le scandale Enron est souvent considéré comme l'archétype de la fraude comptable d'envergure. Cette entreprise américaine spécialisée dans l'énergie, qui a fait faillite en décembre 2001, avait autrefois suscité l'admiration grâce à des états financiers florissants. Pourtant, derrière cette apparence se cachaient des pertes massives et un endettement colossal, largement dissimulés hors bilan. Avec plus de 60 milliards de dollars d'actifs théoriques effacés

lors de sa faillite, l'ascension et la chute d'Enron illustrent la gravité d'une fraude orchestrée au sommet de l'entreprise (Cox, Friedman and Edwards, 2009).

B. Mécanismes de la fraude :

La direction d'Enron, notamment sous l'impulsion du PDG Jeffrey Skilling et du directeur financier Andrew Fastow, a mis en place une fraude comptable sophistiquée. Au cœur de ce mécanisme, l'utilisation d'entités ad hoc (SPV, également appelées SPE) permettait de transférer les actifs dépréciés et de dissimuler les dettes. Ces entités, non consolidées dans les comptes du groupe, servaient à masquer l'ampleur de l'endettement et à présenter des résultats financiers faussement favorables. Par ailleurs, Enron utilisait une méthode agressive de valorisation par le mark-to-market, qui permettait de comptabiliser immédiatement des profits futurs hypothétiques, renforçant ainsi l'illusion d'une performance solide.

C. Détection de la fraude

Des signaux d'alerte avaient pourtant commencé à apparaître dès 2001. Des analystes financiers s'interrogeaient sur le manque de transparence des résultats et une lanceuse d'alerte interne, Sharon Watkins, avait exprimé ses doutes auprès de la direction. Peu à peu, l'incapacité d'Enron à maintenir son « château de cartes » a rendu inévitable la révélation de ses pratiques frauduleuses. En octobre 2001, la société fut contrainte d'annoncer une révision comptable majeure : l'élimination de 618 millions de dollars de bénéfices cumulés et la reconnaissance de 628 millions de dollars de dettes additionnelles, suite à la clôture d'une de ses SPE. Cette révision a attiré l'attention de la SEC, précipitant finalement la faillite de l'entreprise en décembre 2001(‘The fall of enron-palepu healy-2006’, 2006).

D. Conséquences et enseignements :

Le scandale Enron a eu un retentissement mondial en révélant de profondes failles dans le contrôle interne de l'entreprise. Le comité d'audit d'Enron n'avait pas détecté ni compris les montages financiers complexes mis en œuvre par la direction, et la gouvernance défaillante ainsi que les conflits d'intérêts chez l'auditeur externe (le cabinet Arthur Andersen, qui, en outre, avait détruit des documents clés) ont exacerbé la situation. En réponse immédiate à cette affaire, la loi Sarbanes–Oxley (2002) fut instaurée aux États-Unis, imposant notamment la certification annuelle de l'efficacité du contrôle interne par les dirigeants et l'auditeur. Le cas Enron illustre parfaitement une fraude "haut de bilan", initiée par la direction pour tromper les investisseurs et facilitée par la collusion avec l'auditeur externe, tout en utilisant des techniques

complexes, mais finalement détectables par une analyse attentive des flux de trésorerie et des entités liées(Cox, Friedman and Edwards, 2009).

Cet exemple a profondément sensibilisé la communauté financière aux risques de "fraudulent Financial Reporting " et a favorisé l'émergence d'une culture de scepticisme accru en matière d'audit, contribuant ainsi à la mise en place de régulations plus strictes et d'un renforcement des pratiques de gouvernance au sein des entreprises.

1.3.2 Le scandale Parmalat (2003) – Fraude comptable et détournement en collusion (Italie)

A. Contexte et importance du cas :

Parmalat, géant italien de l'agroalimentaire spécialisé dans le lait et ses dérivés, est devenu l'un des exemples les plus retentissants de fraude financière en Europe. Surnommé « l'Enron européen », l'entreprise s'est effondrée fin 2003, laissant derrière elle un trou de 14 milliards d'euros dans ses comptes – la plus grande faillite enregistrée en Europe à cette époque. Ce cas illustre de manière saisissante l'impact des fraudes orchestrées au plus haut niveau et souligne l'importance d'un contrôle interne rigoureux dans les grandes entreprises.(DAVID CHRÉTIEN et JEAN-PIERRE Mabushi , 2007)

B. Mécanismes de la fraude :

La fraude chez Parmalat reposait sur une combinaison complexe de falsification d'états financiers et de détournement d'actifs, opérés en collusion par le fondateur et PDG Calisto Tanzi et ses principaux collaborateurs sur une période de plus d'une décennie.

- Falsification des comptes : Dès les années 1990, Parmalat publiait des états financiers largement falsifiés.

- Création de comptes bancaires fictifs : La direction avait ouvert un prétendu compte à Bank of America aux Îles Caïmans, censé détenir 3,95 milliards d'euros de liquidités, un compte qui s'est avéré inexistant.

- Emission de faux documents : Des lettres de confirmation de solde bancaires falsifiées étaient présentées aux commissaires aux comptes pour attester de l'existence de ces fonds inexistants.

- Montages des sociétés écrans offshore : La fraude s'appuyait également sur un réseau de sociétés écrans, utilisé pour dissimuler des pertes et des dettes en ventilant massivement les emprunts dans des entités hors bilan.

Parallèlement à ces manipulations comptables, des détournements d'actifs ont été pratiqués de manière systématique. Des fonds empruntés par Parmalat auraient servi, entre autres, à financer des investissements personnels et des acquisitions, telles que l'achat d'une équipe de football, permettant à la famille Tanzi de siphonner des ressources hors de l'entreprise.

- **Détection et chute** La situation a commencé à se détériorer lorsque, fin 2003, une échéance obligataire de 150 millions d'euros n'a pu être honorée. Malgré des bilans affichant 4 milliards d'euros de trésorerie, les créanciers, alertés par ce décalage flagrant, ont exigé la vérification de l'encaisse. Le 19 décembre 2003, Bank of America a officiellement démenti détenir des fonds pour Parmalat, révélant que les documents fournis étaient des faux. Cette révélation a précipité l'arrêt des cotations et la mise en faillite de l'entreprise le 24 décembre 2003. Parallèlement, une vaste enquête pénale en Italie a conduit à l'arrestation de Calisto Tanzi, du directeur financier et de nombreux associés impliqués dans la manipulation des comptes et le détournement de fonds.

C. Conséquences et enseignements :

Les retombées du scandale Parmalat ont été considérables. Du point de vue réglementaire, l'affaire a servi de signal d'alarme au niveau européen, renforçant la sensibilisation à la fiabilité des audits et la surveillance des structures financières complexes. Plusieurs banques et cabinets d'audit, dont Grant Thornton et Deloitte, ont été mis en cause pour négligence, certains établissements ayant fermé les yeux sur ces pratiques en percevant d'importantes commissions lors des opérations de refinancement. Calisto Tanzi a ainsi été condamné à de lourdes peines de prison. Malgré cet effondrement, Parmalat a pu être restructurée partiellement et continue d'exister sous une forme réduite(DAVID CHRÉTIEN et JEAN-PIERRE Mabushi, 2007).

Le cas Parmalat illustre de manière concrète comment une fraude comptable de longue haleine, combinée à des détournements orchestrés en collusion, peut prospérer en l'absence de contrôles internes adéquats et d'un scepticisme suffisant de la part des vérificateurs. Il met également en exergue l'importance cruciale de procédures de confirmation indépendantes, puisque la révélation de la fraude reposait en grande partie sur la vérification bancaire externe. Par cet

exemple, la communauté financière a été amenée à repenser ses pratiques de gouvernance et à renforcer ses dispositifs de contrôle pour prévenir la répétition de tels scandales.

1.3.3 Le scandale Wirecard (2020) – Fraude financière et comptable dans une fintech allemande

A. Contexte et Montée en Puissance :

Wirecard était une société allemande de services de paiement en ligne qui, jusqu'en 2019, était considérée comme l'une des étoiles montantes de la fintech européenne. La société affichait une croissance spectaculaire de ses revenus et profits et avait même intégré l'indice boursier DAX en Allemagne. Cependant, en juin 2020, Wirecard s'est effondrée brutalement dans ce qui s'est révélé être un scandale financier mondial, mettant en lumière que près de 1,9 milliard d'euros de trésorerie censés figurer dans ses comptes étaient fictifs.(Gawronsky and Huang, 2024)

B. Mécanismes de la Fraude :

La fraude chez Wirecard reposait sur une combinaison de manœuvres de fraude comptable et de falsification de données financières :

- **Falsification comptable :** Wirecard affichait depuis des années une croissance anormalement soutenue en gonflant artificiellement son chiffre d'affaires et ses liquidités. La direction, dirigée notamment par le CEO Markus Braun et le COO Jan Marsalek, a créé de faux revenus en s'appuyant sur des partenaires tiers complices en Asie et au Moyen-Orient.
- **Dissimulation via des comptes fictifs :** La direction prétendait détenir environ 1,9 milliard d'euros sur des comptes fiduciaires aux Philippines, dispositifs qui, en réalité, n'existaient pas. Deux banques locales étaient censées héberger ces fonds, mais elles ont finalement nié toute interaction et déclaré que les documents fournis s'avéraient être des faux.
- **Utilisation d'entités fictives :** Pour équilibrer son bilan, Wirecard enregistrait d'importants montants de trésorerie inexistants via des filiales et des partenaires, créant ainsi une illusion de solidité financière.
- **Détection et Révélation** Des signaux d'alarme avaient commencé à se faire entendre dès 2019 lorsque des journalistes d'investigation du Financial Times et des vendeurs à découvert émettaient des doutes sur la véracité de certaines activités en Asie. La pression s'est intensifiée en juin 2020, lorsque Wirecard a dû avouer son incapacité à présenter la

preuve de l'existence des 1,9 milliard d'euros manquants. Le 18 juin 2020, le cabinet d'audit EY a refusé de certifier les comptes de l'exercice 2019, affirmant que ces soldes étaient douteux. La révélation a provoqué une chute brutale du cours de Wirecard de plus de 90 % et a précipité la démission, puis l'arrestation du CEO Markus Braun. Quelques jours plus tard, Wirecard a déposé le bilan, laissant derrière elle plus de 4 milliards de dollars de dettes impayées. Parallèlement, Jan Marsalek, alors soupçonné de jouer un rôle central dans la fraude, a pris la fuite, faisant l'objet d'un mandat d'arrêt international. L'enquête a mis au jour l'existence d'un complexe réseau d'entités fictives, implantées notamment à Dubaï et aux Philippines, et a révélé une collusion interne et externe d'une ampleur inattendue.

a) **Conséquences et enseignements** :

L'effondrement de Wirecard a été perçu comme un véritable séisme dans la place financière allemande. Ce scandale a remis en question la fiabilité de la supervision, avec des critiques virulentes adressées au régulateur BaFin, accusé d'inaction voire de protéger l'entreprise. Le rôle de l'auditeur EY a également critiqué pour son incapacité à identifier une fraude aussi complexe malgré plus de dix ans d'audit. Du point de vue réglementaire, l'affaire a conduit à un renforcement des pouvoirs de contrôle en Allemagne et à des réformes dans la gouvernance d'audit. Techniquement, Wirecard illustre une fraude mixte, associant des fausses écritures de revenus et de trésorerie à une falsification externe impliquant des tiers corrompus ou fictifs. Cet exemple souligne l'importance pour les auditeurs de procéder à des confirmations bancaires indépendantes et de rester vigilants face aux signaux d'alerte, notamment quand une entreprise en croissance rapide affiche des montants de trésorerie placés sur des comptes exotiques.

b) **Autres Cas Illustratifs** :

En complément de Wirecard, d'autres scandales tels que le schéma Ponzi de Bernie Madoff (2008), l'affaire Société Générale/Kerviel (2008) et le cas Olympus (2011) ont également enrichi la typologie des fraudes, en mettant en évidence autant des fraudes internes que des détournements et des manipulations comptables. Ces cas ont chacun conduit à des réformes réglementaires et à une amélioration des mécanismes de détection et de prévention.(Reurink, 2016)

Conclusion

Le scandale Wirecard illustre comment une fraude financière et comptable peut être orchestrée au sein d'une entreprise en apparence prospère et comment la supercherie peut perdurer malgré l'audit de longue date. Les mécanismes de manipulation, reposant sur la création de revenus

fictifs et l'utilisation d'entités illusoires, révèlent la nécessité cruciale d'une vérification indépendante des soldes bancaires et d'une vigilance accrue par les régulateurs et les auditeurs. En somme, l'affaire Wirecard rappelle que la fraude, sous toutes ses formes, demeure un défi majeur pour la transparence et la gouvernance d'entreprise, nécessitant une adaptation constante des outils de contrôle et de surveillance pour protéger l'intégrité financière des marchés.

En conclusion, les scandales Enron, Parmalat et Wirecard illustrent les conséquences dévastatrices de la fraude pour les entreprises. Ces cas montrent l'importance de mécanismes de contrôle interne robustes et de la vigilance constante pour détecter et prévenir la fraude. Les leçons tirées de ces exemples doivent guider les pratiques de gouvernance et de contrôle dans les organisations.

Section 2 : Mécanismes de prévention et de détection de fraude

La fraude représente une menace considérable pour les entreprises et les institutions, avec un coût estimé à 2,1 billions de dollars par an à l'échelle mondiale (Galvanize, 2020). Face à cette réalité, les organisations renforcent leurs dispositifs afin de réduire les pertes et protéger leur intégrité financière. Pour ce faire, elles s'appuient sur des cadres réglementaires et normatifs internationaux de référence, tels que :

- COSO, pour structurer le contrôle interne,
- ISO 31000, pour établir un processus robuste de gestion des risques,
- ISA 240 (International Standard on Auditing 240), qui définit précisément la responsabilité des auditeurs en matière de fraude et insiste sur l'importance d'utiliser des procédures analytiques et des tests spécifiques afin de détecter les anomalies dans les états financiers.

De plus, face aux limites des méthodes d'échantillonnage traditionnelles, l'adoption d'outils analytiques performants s'impose. L'analyse de données, par l'examen systématique de l'ensemble des transactions, permet d'identifier des tendances, des schémas suspects et des irrégularités, offrant ainsi une couverture complète qui réduit le risque de transactions frauduleuses passées inaperçues. Les mécanismes de prévention tendent avant tout à réduire les opportunités de fraude. Cela se traduit par le renforcement des contrôles internes, la mise en œuvre de systèmes de surveillance proactive et une politique active de sensibilisation des employés aux risques. Parallèlement, l'efficacité des outils de détection repose sur l'utilisation

de techniques d'analyse de données avancées, qui permettent de repérer rapidement toute anomalie dans les opérations financières.

En définitive, ce point présente une approche intégrée où la combinaison des cadres normatifs internationaux (COSO, ISO 31000, ISA 240) et l'essor des technologies d'analyse de données contribuent à structurer un programme de lutte contre la fraude à la fois complet et efficace. Un leadership éthique et un engagement affirmé de la direction restent également des éléments déterminants dans la réussite de ces stratégies.

2. Stratégies globales de prévention de la fraude

Les organisations capables de maîtriser le risque de fraude adoptent une démarche proactive et intégrée, qui repose sur des cadres référentiels normatifs internationaux reconnus. Ces stratégies visent à limiter les opportunités de fraude et à renforcer la vigilance à tous les niveaux de l'entreprise.

2.1 Renforcement du contrôle interne

Selon le cadre COSO, un système de contrôle interne efficace constitue la première ligne de défense contre la fraude. Ce renforcement débute par :

2.1.1 Création d'un environnement de contrôle solide

- Mise en place d'un code de conduite formellement établi et diffusé auprès de tous les employés
- Adoption d'une politique de tolérance zéro envers la fraude
- Engagement visible de la direction en faveur d'une éthique rigoureuse

2.1.2 Intégration de contrôles spécifiques anti-fraude dans les procédures opérationnelles

- Séparation des pouvoirs pour les transactions financières (aucune personne ne doit pouvoir à la fois initier et approuver un paiement)

- Contrôle des accès aux systèmes sensibles (droits limités et régulièrement révisés) ;

- Validations multiples pour les écritures comptables inhabituelles ;

- Rapprochements fréquents (banque, stock) pour identifier rapidement les écarts.

2.1.3 Adaptation continue et mise en place de programmes anti-fraude dédiés

- Évaluation régulière des changements (principe 9 du COSO) afin de réévaluer les risques lors de modifications de processus ou d'organisation
- Déploiement d'un plan de prévention et de détection incluant la formation des employés, la rotation des postes à risque, l'analyse des données transactionnelles (data analytics), et des protocoles d'enquête interne en cas de suspicion

Le guide COSO-ACFE vient compléter ces recommandations en insistant sur le dépistage proactif à l'aide d'outils informatiques et la création d'une fonction dédiée à la fraude ou d'un comité antifraude pour superviser l'ensemble du programme.

1.2.2 Évaluation Régulière et Gestion du Risque de fraude

En s'inspirant de la norme ISO 31000, les organisations doivent instaurer un processus continu de gestion du risque de fraude

- Évaluations périodiques :
- Réaliser au moins une évaluation annuelle de l'ensemble des activités ;
- Identifier les scénarios de fraude pertinents, évaluer leur probabilité et leur impact, et prioriser les mesures correctives ;
- Stratégies de traitement adaptées ;
- Renforcer les contrôles internes lorsque le risque résiduel est trop élevé ;
- Transférer une partie du risque via des assurances (ex. assurance contre la malhonnêteté des employés ou assurance crime) ;
- Accepter de manière raisonnée certains risques mineurs ;
- · Communication et formation :
    - Sensibiliser régulièrement l'ensemble du personnel via des sessions de formation, des modules e-learning sur l'éthique et la fraude, et des rappels des procédures de signalement,
    - Suivre rigoureusement les incidents de fraude (documentation, analyse, reporting et retour d'expérience auprès de la gouvernance) ;

- Conformité à ISA 240 et Renforcement du Rôle de l'Audit cette section se divise en plusieurs sous-parties :

  - Présentation de la norme ISA 240 : L'ISA 240 regroupe les normes internationales d'audit consacrées à la fraude. Elle précise les responsabilités des auditeurs dans l'identification et l'évaluation des fraudes, ainsi que les prérogatives et la méthodologie à suivre.

  Selon les travaux de Haryanto et Ardilla en 2022, le renforcement de l'audit interne et externe est crucial pour lutter contre la fraude. Voici quelques mesures recommandées :

- Auditeur externe :

  - Organiser des séances de brainstorming sur le risque de fraude.
  - Réaliser des tests ciblés sur le journal comptable et les ajustements en clôture.
  - Contrôler les revenus et d'autres aspects financiers sensibles

- Surveillance interne :

  - Examiner régulièrement des revues d'écritures inhabituelles pour détecter et corriger les anomalies avant l'audit externe.

  - Collaboration entre Audit Interne et Audit Externe :

  - Partager des informations sur les zones de risque.

  - Communiquer sur les faiblesses de contrôle détectées afin d'assurer une correction durable.

  - Mesures pour Renforcer l'Audit Interne dans la Détection de la Fraude :

  - Intégrer des missions spécifiques axées sur le risque de fraude dans le plan d'audit (audits de conformité, audits ciblés sur les paiements sensibles et les stocks, etc.).

  - Développer les compétences des auditeurs internes par des formations spécialisées ou par le recrutement de profils experts (certification CFE, analytique de données, forensic).

  - Utiliser des outils d'analyse performants (logiciels d'extraction de données pour détecter des doublons, des fournisseurs inhabituels ou des schémas anormaux).

- Établir un protocole de coordination avec les fonctions juridique, compliance et RH pour le traitement des suspicions de fraude.
- Assurer le suivi des recommandations de contrôle par un plan d'action concret pour chaque faiblesse identifiée.

En conclusion, les organisations qui maîtrisent le risque de fraude adoptent une démarche intégrée et proactive. Elles mobilisent toutes les lignes de défense, s'appuient sur des cadres reconnus (COSO, ISO 31000, ISA 240) et investissent dans des outils spécifiques (formation, systèmes d'alerte, analyses de données, équipes dédiées). Le leadership éthique et l'engagement de la direction constituent également des facteurs clés pour réussir ces stratégies.

Il est également à noter que, bien que les audits et contrôles internes soient essentiels pour identifier les activités frauduleuses, les méthodes traditionnelles basées sur l'échantillonnage présentent certaines limites. En effet, elles ne permettent pas d'analyser systématiquement l'ensemble des transactions, risquant ainsi de passer à côté d'anomalies répétitives. L'essor des technologies d'analyse de données apparaît alors comme une solution complémentaire indispensable.

1.3. Détection et Prévention de la Fraude par l'Analyse de Données

Parallèlement aux stratégies globales de prévention, l'analyse de données offre une approche innovante en permettant d'examiner l'intégralité des transactions pour identifier des irrégularités susceptibles d'échapper aux méthodes d'échantillonnage traditionnelles. Cette technologie permet une couverture totale, réduisant significativement le risque de passer à côté de transactions frauduleuses. Plusieurs techniques analytiques, dont le développement sera détaillé dans une section ultérieure, permettent ainsi de repérer des tendances, des schémas suspects et des anomalies dans les opérations financières.

3.1 Lois et Principes Statistiques Appliqués à la Détection de Fraude

Selon les travaux de Benford (1938), Bernoulli (1713), et Gauss (1809), les lois statistiques jouent un rôle crucial dans l'analyse des données financières pour détecter les irrégularités et les fraudes. Voici quelques points clés :

Loi de Benford :

- Distribution des chiffres : Le chiffre "1" apparaît en première position environ 30 % du temps, tandis que le chiffre "9" apparaît moins de 5 % du temps.

- Détection de fraude : Une déviation notable de cette répartition peut indiquer une manipulation frauduleuse, souvent utilisée pour déceler des ajustements comptables abusifs ou des fraudes fiscales.

Loi des grands nombres :

- Échantillons larges : Un échantillon suffisamment large devrait refléter fidèlement la moyenne attendue.
- Signes de fraude : Une variable qui s'écarte significativement de sa moyenne habituelle sur un vaste ensemble de données peut signaler une possible fraude.

Loi normale (distribution gaussienne) :

- Répartition des valeurs : Environ 68 % des valeurs se situent à un écart-type de la moyenne, 95 % à deux écarts-types, et 99,7 % à trois écarts-types.
- Outliers : Les transactions qui se trouvent en dehors de ce spectre habituel peuvent constituer des indices forts d'anomalie, nécessitant une investigation plus approfondie.

Ces lois fournissent des outils puissants pour l'analyse statistique en finance, aidant à identifier des anomalies qui pourraient indiquer des fraudes.

3.2 Ratios Analytiques pour Détecter la Fraude

Selon les travaux de Kochinev, Antysheva, et Putintseva (2020), l'analyse des ratios financiers offre un moyen complémentaire de scruter l'activité d'une entreprise en comparant divers indicateurs clés. Voici quelques points importants :

Analyse des ratios financiers :

- Évaluation des risques : Les ratios financiers permettent d'évaluer les risques de fausse déclaration matérielle dans les états financiers en raison de la fraude.
- Indicateurs clés : Comparer divers indicateurs financiers pour détecter des anomalies ou des irrégularités.

Procédures analytiques formalisées :

- Procédures d'audit : Formalisation des procédures analytiques pour évaluer les risques de fausse déclaration matérielle.

- Conférence scientifique : Présentation des résultats lors de la 2ème Conférence Scientifique Internationale sur les Innovations dans l'Économie Numérique (SPBPU IDE-2020).

Ainsi, le ratio Maximum/Minimum, qui évalue l'écart entre les valeurs extrêmes d'un ensemble de transactions, peut s'avérer particulièrement révélateur : une variation anormalement large peut indiquer soit des paiements frauduleux, soit une manipulation artificielle des comptes.

Un autre ratio tout aussi instructif est celui des Transactions Répétées. En mesurant la fréquence des transactions identiques ou similaires – souvent réalisées par les mêmes parties à des intervalles irréguliers – ce ratio permet de repérer des doublons ou des répétitions anormales, comme lorsqu'une facture est indûment payée plusieurs fois à un même fournisseur.

Le Ratio de Croissance des Dépenses constitue également un indicateur robuste. Il met en lumière toute augmentation soudaine et dénuée d'explications plausibles des dépenses sur une période donnée. Lorsqu'une hausse significative est observée, cela peut trahir des détournements de fonds ou des fraudes internes.

Pour aller encore plus loin, le Ratio d'Activité par Employé compare le nombre de transactions générées par chaque collaborateur à la moyenne globale. Si un employé se démarque par une activité bien supérieure à celle de ses pairs, cela pourrait signaler des comportements suspicieux, tels que la création de fausses factures.

Enfin, le Ratio de Variation des Montants Unitaires met en lumière les écarts de prix entre deux périodes. Un ajustement important, inexplicable par les conditions de marché, peut alors être interprété comme une preuve potentielle de fraude sur les prix de facturation.

3.3 Vers une Supervision Continue et Automatisée

L'un des aspects les plus prometteurs dans la lutte contre la fraude repose sur la capacité des systèmes d'analyse de données à fonctionner en continu. En intégrant des tests automatisés, il devient possible de détecter en temps réel toute anomalie, réduisant ainsi l'intervalle entre la survenue de la fraude et sa détection. L'utilisation de solutions basées sur l'intelligence artificielle et le machine Learning permet, quant à elle, d'affiner les modèles de détection et de minimiser les faux positifs (Vanini et al,2023). Cette approche dynamique assure une surveillance permanente, garantissant que les anomalies ne passent pas inaperçues.

3.4 Mise en Place d'un Programme de Détection et de Prévention de la Fraude :

La mise en œuvre d'un programme de lutte contre la fraude, intégrant l'analyse de données, repose sur une démarche méthodique en plusieurs étapes clés(Chen *et al.*, 2025) :

- **Identification des risques :** Il s'agit ici de recenser l'ensemble des types de fraude potentiels et d'étudier précisément les domaines les plus exposés.
- **Évaluation des pertes potentielles :** La quantification des impacts financiers, en l'absence de contrôles adéquats, permet de prioriser les efforts de prévention.
- **Développement de tests analytiques ciblés :** L'élaboration d'indicateurs et de modèles de détection adaptés à chaque risque spécifique est essentielle pour cibler les anomalies pertinentes.
- **Supervision continue :** L'automatisation de la surveillance via des workflows d'alerte offre une capacité de réaction rapide, garantissant une vigilance constante.
- **Renforcement des contrôles internes :** Enfin, l'amélioration des politiques internes et la sensibilisation des parties prenantes à la problématique de la fraude viennent compléter ce dispositif.

4. Qualification du Risque de Fraude Interne dans une Entreprise :

Le risque, défini comme une incertitude susceptible d'affecter négativement une entreprise, un projet ou un individu, peut provenir tant d'un environnement interne (erreurs humaines, fraudes, mauvaise gestion) que d'un contexte externe (crises économiques, cyberattaques, catastrophes naturelles). L'évaluation de ce risque repose sur l'analyse approfondie de sa nature, de sa probabilité d'occurrence et de son impact potentiel sur les activités, les ressources et les objectifs visés. Il s'agit d'une démarche méthodique permettant d'identifier les facteurs de risque, de mesurer leur ampleur et d'anticiper leurs conséquences, afin de mettre en place des stratégies de prévention et d'atténuation adaptées.

4.1 Le Risque de Fraude Interne :

Le risque de fraude interne est défini, selon l'IFAC, comme « le risque qu'un acte intentionnel soit commis par une ou plusieurs personnes au sein de la direction, parmi les membres du gouvernement d'entreprise, les employés ou des tiers, utilisant la ruse pour obtenir un avantage

injuste ». En d'autres termes, la fraude interne recouvre l'ensemble des actes malhonnêtes réalisés par des employés ou dirigeants dans le but de tirer un avantage personnel au détriment de l'entreprise. Des études (Poels and Zawadzki, 2013) indiquent que ce type de fraude peut représenter jusqu'à 5 % du chiffre d'affaires des entreprises.

Pour mieux qualifier ce risque, plusieurs dimensions peuvent être distinguées :

a. Risque Opérationnel Ce risque concerne les perturbations affectant directement le fonctionnement quotidien de l'entreprise. Il résulte généralement d'une mauvaise gestion des ressources, de contrôles internes défaillants ou d'un manque de vigilance dans les processus opérationnels, compromettant ainsi la capacité de l'entreprise à livrer ses produits et services dans les délais et selon les standards de qualité attendus.
b. Risque Financier Il découle des fraudes qui impactent les flux monétaires de l'entreprise, telles que le détournement de fonds, les fausses facturations ou encore la manipulation comptable. Ce risque entraine des pertes financières directes pouvant compromettre la santé économique de l'organisation.
c. Risque Juridique et Réglementaire Une fraude interne peut entraîner une violation des lois et des réglementations en vigueur. Cela expose l'entreprise à des poursuites judiciaires, à des sanctions administratives et à des amendes, compromettant la légalité de ses opérations. Dans les cas extrêmes, une telle violation pourrait même conduire à la dissolution de l'entreprise.
d. Risque de Réputation La réputation constitue un atout stratégique majeur pour toute entreprise. La révélation d'une fraude interne peut gravement ternir l'image de l'organisation, érodant la confiance des clients, des partenaires et des investisseurs, et ayant ainsi des répercussions durables sur sa position sur le marché.
e. Risque Stratégique Les fraudes internes peuvent fausser les décisions stratégiques en fournissant des informations erronées sur la performance réelle de l'entreprise. Par exemple, un dirigeant pourrait manipuler les données de performance pour masquer des pertes et éviter d'attirer l'attention des actionnaires. Les conséquences de ce risque se manifestent notamment par une mauvaise allocation des ressources, une prise de risque excessive en l'absence d'une vision claire de la situation réelle, et un impact négatif sur la gouvernance et la crédibilité des dirigeants auprès des investisseurs et des organes de contrôle (Reurink, 2016).

Section 03 : contrôle interne

3.1. Historique et évolution

" Le contrôle interne ? Il vient de loin, du fond de notre histoire. Le premier homme préhistorique qui allumait un feu à l'entrée de sa caverne agissait pour se prémunir contre un risque : celui de l'attaque des bêtes sauvages. Et, ce faisant, il mettait en place un dispositif de contrôle interne ... „(*Jacques Renard, 2011*) .

Ainsi, historiquement les premières civilisations, sans en avoir conscience, mettaient déjà en place des formes rudimentaires de contrôle interne. Le chef de tribu qui sécurise son territoire, l'artisan qui organisait ses outils pour éviter le gaspillage, le marchand qui vérifiait ses transactions : tous appliquent instinctivement des principes de maîtrise et de protection, il s'agissait d'un contrôle interne intuitif.

Mais il fallut attendre le XXe siècle pour que ces pratiques intuitives deviennent une discipline à part entière.

L'émergence du concept (1940-1960) : une origine anglo-saxonne

Dans les années 1940, les comptables anglo-saxons, en particulier les experts américains de l'American Institute of Certified Public Accountants (AICPA), introduisirent le concept de '"nternal Control". Une erreur de traduction fit alors naître une confusion en France : le terme fut interprété comme une simple vérification, alors qu'il s'agissait avant tout d'une démarche de maîtrise et de structuration des opérations (Berland ,1998).

Au même moment, des auteurs comme Lawrence Sawyer (États-Unis, 1911-2002), l'un des pionniers de l'audit interne, commencèrent à structurer cette discipline. Il affirma que l'audit interne et le contrôle interne étaient indissociables, l'un étant le garant de l'efficacité de l'autre.

Dans les années 1960, la France adopta progressivement ce concept. L'Ordre des experts-comptables et la Compagnie nationale des commissaires aux comptes (CNCC) mirent en avant l'idée que le contrôle interne pouvait garantir la fiabilité des états financiers et minimiser les erreurs. Toutefois, cette approche restait principalement orientée vers la comptabilité.

3.2. La structuration du contrôle interne (1970-1980) : vers une vision élargie

Les années 1970 marquèrent une évolution majeure. En 1977, l'Ordre des experts-comptables français élabora une définition élargie du contrôle interne, mettant en avant son rôle dans la préservation du patrimoine et la qualité de l'information financière. La même année, le Consultative Committee of Accountancy au Royaume-Uni publia une définition similaire, confirmant la tendance à considérer le contrôle interne comme un levier de gouvernance et de performance.

Un autre acteur joua un rôle clé : Robert K. Elliott (États-Unis), un expert en audit et contrôle interne, qui participa aux discussions sur la nécessité d'un cadre structuré pour guider les entreprises.

Les années 1990 : la naissance des grands référentiels

Mais ce n'était encore que le début. Les années 1980 virent une montée des scandales financiers à travers le monde tel que le Scandale Enron, Scandale de la banque Baring…. Celles-ci révèlent les failles des systèmes de contrôle interne. Aux États-Unis, le sénateur James C. Treadway (États-Unis) dirigea une enquête approfondie, ce qui a débouché sur en 1992 à la création du référentiel COSO 1 (Committee of Sponsoring Organizations of the Treadway Commission) au-delà de son origine et son histoire la COSO est un organisme américain qui élabore des référentiels qui est largement utilisé par les entreprises permettant d'améliorer le contrôle interne et la gestion des risques et la gouvernance des entreprises ils structure cette dernière selon cinq composantes :

- L'environnement de contrôle
- L'évaluation des risques
- Les activités de contrôle
- L'information et la communication
- La supervision

Le COSO 1 fut rapidement adopté à l'échelle internationale et inspira de nombreux référentiels, notamment le CoCo (Canada) en 1995, développé par le Comité sur les critères de contrôle (CoCo) et le Turnbull Guidance (Royaume-Uni, 1999).

Les années 2000 : le renforcement après les scandales

Le début des années 2000 fut marqué par des crises financières majeures, comme les faillites aux États-Unis. Ces événements dramatiques mirent en évidence les failles des dispositifs de contrôle interne et entraînèrent l'adoption de lois plus strictes :

- Le Sarbanes-Oxley Act (SOX, 2002, États-Unis), porté par les sénateurs Paul Sarbanes et Michael Oxley, imposa des obligations accrues en matière de contrôle interne aux entreprises cotées.
- En France, la Loi sur la Sécurité Financière (LSF, 2003) a imposé aux entreprises de renforcer leur gouvernance et leur transparence financière.

Durant cette période, le COSO 2 (2004) vit le jour, intégrant une approche plus orientée vers la gestion des risques. En parallèle, en France, l'Autorité des marchés financiers (AMF) publia en 2006 un référentiel national de contrôle interne adapté au contexte réglementaire français.

Depuis 2010 : une évolution continue vers la gestion globale des risques

Aujourd'hui, le contrôle interne ne se limite plus aux aspects financiers. Il englobe désormais des thématiques essentielles comme :

- La cybersécurité : encadrée par des régulations comme le RGPD (Règlement Général sur la Protection des Données, 2018).
- La responsabilité sociétale des entreprises (RSE) : les entreprises sont appelées à intégrer des critères environnementaux et sociaux dans leurs dispositifs de contrôle.
- La lutte contre la fraude et la corruption : avec des lois comme Sapin II (2016, France) et le Foreign Corrupt Practices Act (FCPA, États-Unis).

Des experts comme **Jacques Renard (France)**, auteur du livre Comprendre *et mettre en œuvre le contrôle interne*, continuent d'apporter des méthodologies pour perfectionner ces systèmes et les adapter aux enjeux modernes.

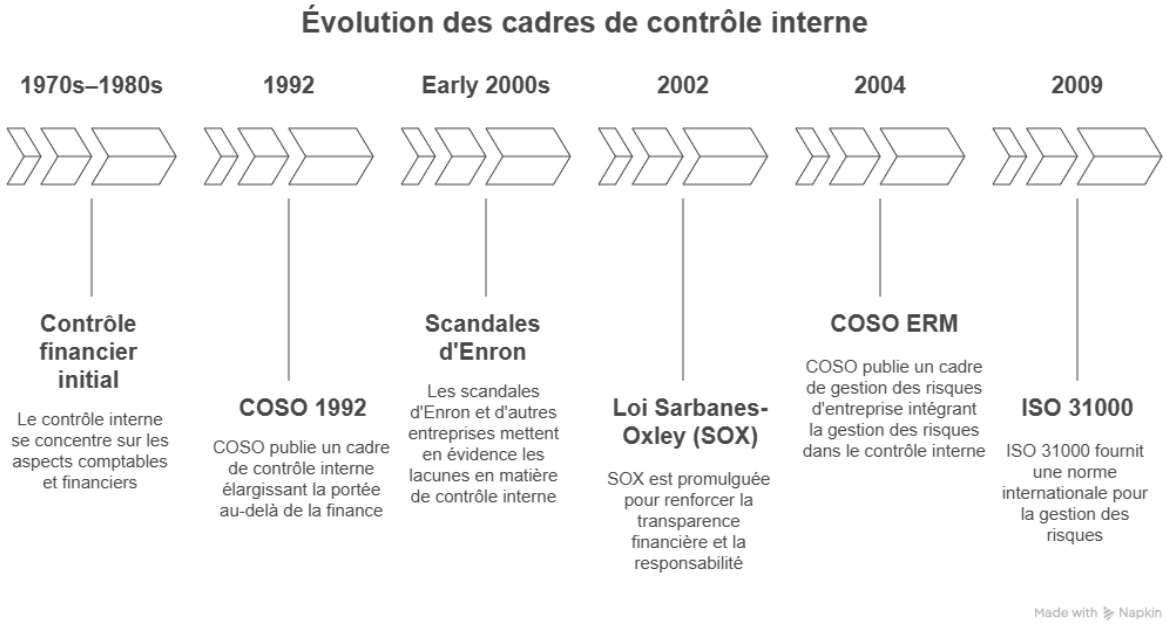
Conclusion : une évolution sans fin

L'histoire du contrôle interne est celle d'une adaptation constante aux défis de son époque. D'un simple concept comptable, il est devenu un outil fondamental de gouvernance et de gestion des risques. Des premiers travaux des comptables anglo-saxons aux référentiels modernes comme

le COSO et le RGPD, il n'a cessé d'évoluer pour répondre aux crises et aux transformations du monde économique.

Et l'histoire continue de s'écrire…

Figure 2 : Figure récapitulative de l'évolution du contrôle interne.



Source : (Frédéric Bernard,Rémi Gayraud, Laurent Rousseau, 2008)

3.3. Définition et composante du contrôle interne :

Le contrôle interne se définit comme l'ensemble des processus, politiques et pratiques mis en œuvre par une organisation pour assurer la fiabilité de ses informations financières, l'efficacité de ses opérations et le respect des lois, tout en protégeant ses actifs contre les risques et la fraude (Henk, 2020). Au cœur de cette démarche, plusieurs référentiels fournissent des cadres conceptuels robustes et complémentaires.

Selon le **COSO (Committee of Sponsoring Organizations of the Treadway Commission)** le contrôle interne est défini comme un processus intégré et dynamique qui englobe la clôture, la structure et les taches conçues pour fournir une assurance raisonnable quant à la réalisation des objectifs organisationnels suivants :

- Réalisation et optimisation des opérations ;

- Fiabilité des informations financières ;
- Conformité aux lois et aux réglementations en vigueur.

Le modèle COSO, l'un des cadres les plus influents, définit le contrôle interne à travers cinq composantes fondamentales résumé dans le schéma qui suit :

Environnement de contrôle

- Base fondamentale : reflète la culture d'éthique, les valeurs et l'engagement de la direction.
- Inclut des principes clairs de gouvernance et une structure organisationnelle adaptée.

Évaluation des risques

- Permet d'identifier, analyser et hiérarchiser les risques susceptibles d'affecter l'entreprise.
- Aide à mettre en place des mesures adaptées pour atténuer ces menaces.

Activités de contrôle

- Ensemble des politiques et procédures destinées à réduire les risques identifiés.
- Inclut des vérifications régulières, des autorisations et des processus de supervision.

Information et communication

- Garantit une diffusion efficace et fiable des informations pertinentes à l'interne comme à l'externe.
- Permet d'appuyer la prise de décision grâce à des données claires et transparentes.

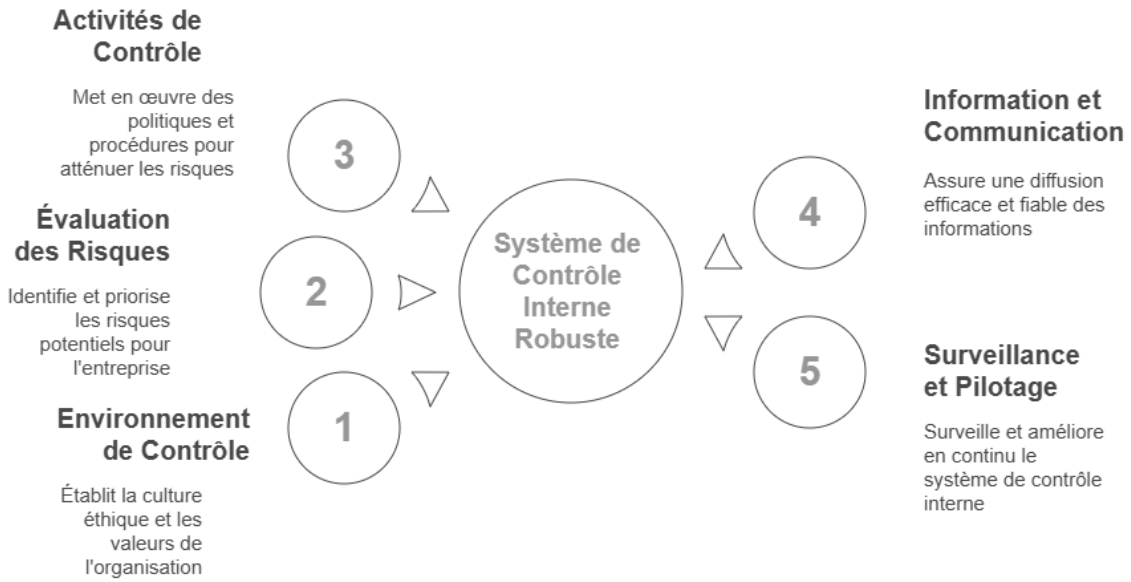
Surveillance et pilotage

- Assure un suivi continu du dispositif de contrôle interne et son amélioration.
- Comprend les audits internes et les évaluations périodiques pour ajuster le système en fonction des évolutions.

Chaque composante agit de manière interconnectée pour offrir un dispositif cohérent et robuste, essentiel à la durabilité et à la performance d'une organisation.

Pour une meilleure compréhension des composantes abordées, celles-ci sont résumées dans le schéma ci-dessus.

Figure 3 : Composants d'un système de contrôle interne robuste



Source : Frédéric Bernard,Rémi Gayaraud,Laurent Rousseau, 2008)

Dans le prolongement de cette approche, l'Enterprise Risk Management (ERM), tel qu'intégrable dans le cadre COSO ERM (2004), élargit la notion de contrôle interne. Il s'agit ici d'un outil proactif, in2007tégré à la gestion globale des risques, qui facilite non seulement la prévention et la correction des défaillances, mais aussi l'anticipation des menaces et l'optimisation des opportunités pour la stratégie de l'entreprise.

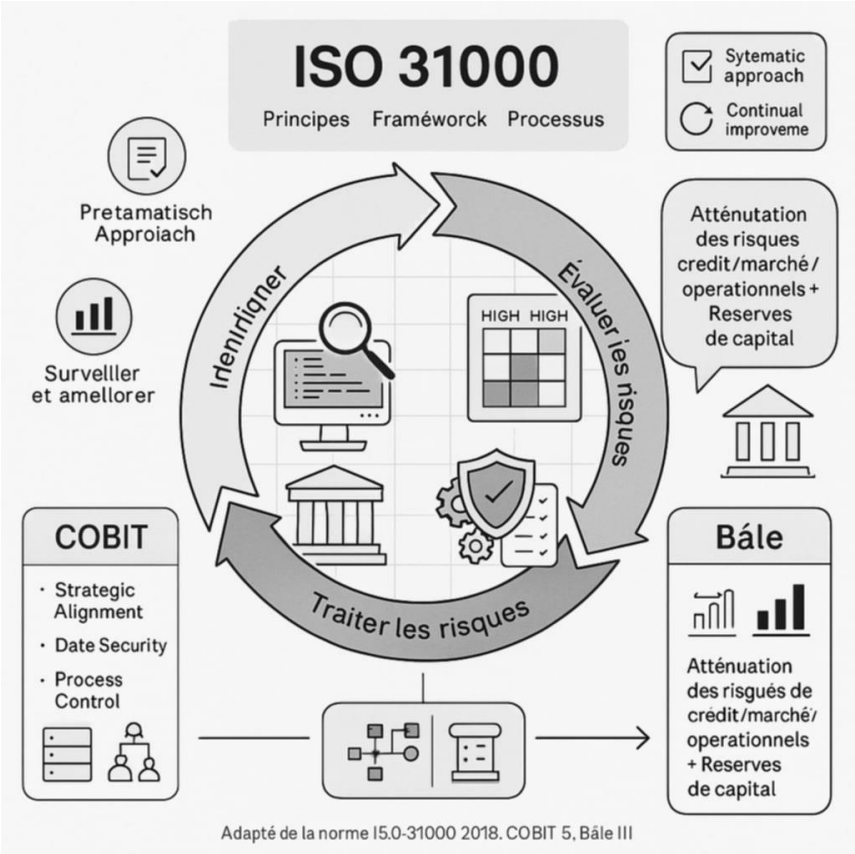
Par ailleurs, la Fédération Internationale des comptables (IFAC, 2010) insiste sur le fait qu'un contrôle interne efficace ne se réduit pas uniquement à la vérification des chiffres. Il doit également promouvoir l'intégrité et l'indépendance des professionnels, intégrant ainsi des valeurs éthiques essentielles dans les pratiques quotidiennes. Cette vision met l'accent sur le rôle du contrôle interne en tant que vecteur de gouvernance et de transparence au sein de l'organisation.

La norme ISO 31000 (publiée initialement en 2009 et mise à jour en 2018) complète cette approche en proposant un cadre systématique pour la gestion des risques. Dans cette optique, le contrôle interne joue un rôle fondamental en fournissant des informations fiables sur les risques, facilitant l'implémentation d'actions correctives dans un cycle permanent d'amélioration.

Axes clés selon l'ISO 31000 :

Figure les composantes clés de la norme ISO 31000

Figure 4 : Cadre intégré de gestion des risques : ISO 31000, Cobit Basel



Source :la norme ISO 31000

Pour le domaine des technologies de l'information, COBIT (avec COBIT 4.1 en 2007 et COBIT 5 en 2012) propose une approche spécifique qui assure la gouvernance et le contrôle des systèmes informatiques, garantissant notamment la sécurité, la conformité et la performance des données critiques en alignant les processus IT sur les objectifs stratégiques de l'entreprise.

Ses objectifs :

- **Alignement stratégique** des ressources IT avec la stratégie globale de l'entreprise.
- **Contrôle des systèmes d'information** pour assurer sécurité, conformité et fiabilité des données.

- **Gestion des processus IT** pour prévenir les risques techniques et informatiques.

En outre, dans le secteur financier, les recommandations du Comité de Bâle (avec Basel II en 2004 et Basel III en 2010) soulignent l'importance d'un contrôle interne rigoureux pour la gestion des risques de crédit, de marché et opérationnels. Ces normes exigent des dispositifs de surveillance sophistiqués et des niveaux adéquats de réserves de capital, assurant ainsi la stabilité et la résilience des institutions financières.

À ces cadres établis s'ajoutent d'autres définitions importantes. Par exemple, le référentiel COCO (Committee on Corporate Oversight) met en avant que le contrôle interne doit également favoriser une gouvernance efficiente et la conformité aux obligations réglementaires, en s'attachant à la qualité du reporting et à l'amélioration continue des processus. COCO met davantage l'accent sur la culture organisationnelle et l'importance des valeurs.

Ses quatre éléments :

1. **Définir des objectifs clairs**.
2. **Identifier les engagements et responsabilités de chacun.**
3. **Mettre en œuvre des contrôles appropriés aux processus opérationnels.**
4. **Surveiller et ajuster les pratiques régulièrement.**

La Loi Sarbanes–Oxley (Section 404, USA, 2002) renforce cette exigence en imposant aux entreprises publiques de fournir chaque année des attestations rigoureuses sur la qualité de leur contrôle interne, afin de restaurer la confiance des investisseurs. De plus, le Public Company Accounting Oversight Board (PCAOB), en parallèle avec la Loi Sarbanes–Oxley, impose des normes strictes aux cabinets d'audit et à leurs audits, garantissant ainsi que le contrôle interne soit évalué de manière indépendante et fiable.

En somme, le contrôle interne, tel que défini par ces divers référentiels internationaux – COSO, ERM, IFAC, ISO 31000, COBIT, ainsi que par la Loi Sarbanes–Oxley, le COCO et le PCAOB – apparaît comme un système intégré et dynamique. Ce dispositif combine des mécanismes techniques de vérification, une gestion proactive des risques et une forte dimension éthique et de gouvernance, essentiels pour assurer la fiabilité des informations financières et la pérennité des organisations. Cette approche multidimensionnelle est fondamentale pour transformer les

incertitudes en opportunités et pour instaurer une culture d'intégrité et de responsabilité indispensable à la compétitivité des entreprises sur le long terme.

Analyse comparative des référentiels de contrôle interne :

Dans ce travail, nous examinons les différentes approches du contrôle interne selon les principaux référentiels internationaux, tels que COSO, COCO, IFAC, la Loi Sarbanes–Oxley (SOX) et le PCAOB, ainsi que les cadres dédiés à la gestion des risques comme l'ERM et ISO 31000. Nous intégrons également les perspectives spécifiques de COBIT pour la gouvernance IT et les recommandations du Comité de Bâle pour le secteur financier.

L'objectif de cette analyse est double : mettre en lumière les points communs entre ces référentiels et identifier leurs différences en termes de périmètre, d'accent et de finalité. Par ailleurs, nous soulignons comment ces approches, parfois complémentaires, peuvent contribuer à instaurer une gouvernance partagée, permettant non seulement de protéger les actifs et d'assurer la fiabilité des informations, mais aussi de transformer les incertitudes en leviers stratégiques dans un environnement complexe et en constante évolution.(Henk, 2020)

Principes communs Les référentiels convergent sur plusieurs notions fondamentales :

- **Processus intégré et participatif** : Le contrôle interne est un dispositif dynamique impliquant à la fois la direction et l'ensemble du personnel, garantissant une assurance raisonnable quant à l'atteinte des objectifs organisationnels.
- **Objectifs clés** : Les principaux objectifs incluent l'efficacité des opérations, la fiabilité des informations financières et la conformité aux lois et règlements.
- **Responsabilité collective** : Au-delà de la fonction d'audit, le contrôle interne est vu comme un engagement partagé entre toutes les parties prenantes de l'organisation.

Différences de périmètre et d'accent Bien que les référentiels partagent des bases communes, leurs orientations varient :

- **Vision holistique vs. Spécifique** : Des cadres comme COSO, COCO et ISO 31000 abordent le contrôle interne de manière globale, intégrant tous les processus et risques de l'entreprise, tandis que SOX et PCAOB se concentrent principalement sur la fiabilité comptable et financière.

- **Finalité recherchée** : Les régulateurs financiers (ex. SOX) mettent l'accent sur la transparence financière pour les investisseurs, tandis que les instances de gouvernance (COSO, ISO 31000) voient le contrôle interne comme un levier de performance opérationnelle et stratégique.
- **Dimension culturelle** : Alors que COCO intègre explicitement la culture et les facteurs humains, COSO aborde ces aspects de façon plus indirecte à travers l'environnement de contrôle.

Orientations spécifiques : gestion des risques et contrôle financier Les référentiels adoptent différentes approches pour aborder le contrôle interne :

- **Approche "Top-down" (gestion des risques)** : COSO ERM et ISO 31000 intègrent le contrôle interne dans un cadre de gestion des risques, orienté vers l'identification et la prévention des menaces stratégiques.
- **Approche "Bottom-up" (contrôle financier)** : COBIT et PCAOB privilégient une mise en œuvre précise des contrôles comptables et opérationnels afin de sécuriser les processus critiques.
- **Dimension duale** : Certains référentiels mettent l'accent sur le « pourquoi » du contrôle interne (répondre aux risques), tandis que d'autres se concentrent sur le « comment » (procédures détaillées).

Évolutions historiques et convergence des normes Le contrôle interne a évolué au fil du temps pour s'adapter aux besoins des organisations :

- **Développement initial** : Dans les années 1970–80, il était principalement centré sur les aspects comptables et financiers.
- **Élargissement** : Depuis COSO 1992 et les scandales comme Enron, il englobe désormais les processus opérationnels et la conformité.
- **Intégration des risques** : Avec l'émergence de COSO ERM et ISO 31000, la gestion des risques est devenue un axe stratégique du contrôle interne.
- **Uniformisation internationale** : Les cadres globaux (COSO, ISO 31000) favorisent un langage commun, tout en permettant des adaptations sectorielles comme celles du Comité de Bâle pour le secteur bancaire ou COBIT pour les systèmes IT.

Afin de mieux comprendre les différentes approches du contrôle interne selon les principaux référentiels internationaux, nous avons synthétisé les informations clés dans le tableau ci-dessous. Ce tableau met en lumière les points communs et les différences en termes de périmètre, d'accent et de finalité, tout en soulignant les orientations spécifiques de chaque référentiel.

Référentiel	**Périmètre**	**Accent principal**	**Finalité recherchée**	**Dimension culturelle**	**Approche spécifique**
COSO	Global	Tous les processus et risques	Performance opérationnelle et stratégique	Indirecte via l'environnement de contrôle	Gestion des risques (Top-down)
COCO	Global	Tous les processus et risques	Performance opérationnelle et stratégique	Intègre explicitement la culture et les facteurs humains	Gestion des risques (Top-down)
IFAC	Comptable et financier	Fiabilité des informations	Transparence financière	Non spécifié	Contrôle financier (Bottom-up)
SOX	Comptable et financier	Fiabilité comptable et financière	Transparence financière pour les investisseurs	Non spécifié	Contrôle financier (Bottom-up)
PCAOB	Comptable et financier	Fiabilité comptable et financière	Transparence financière	Non spécifié	Contrôle financier (Bottom-up)

ERM	Global	Gestion des risques	Performance stratégique	Non spécifié	Gestion des risques (Top-down)
ISO 31000	Global	Gestion des risques	Performance stratégique	Non spécifié	Gestion des risques (Top-down)
COBIT	IT	Gouvernance IT	Sécurisation des processus critiques	Non spécifié	Contrôle financier (Bottom-up)
Comité de Bâle	Secteur financier	Régulation bancaire	Stabilité financière	Non spécifié	Gestion des risques (Top-down)

Tableau 1 : Comparaison des référentiels de contrôle interne et de gestion des risques : périmètre, finalités et approches

En conclusion, malgré des différences dans leur périmètre et leurs priorités, les référentiels convergent vers un fondement commun : le contrôle interne est un dispositif intégré et participatif, essentiel à la maîtrise des risques et à l'atteinte des objectifs organisationnels. Cette approche multidimensionnelle permet aux entreprises de renforcer leur compétitivité, d'assurer leur pérennité et de promouvoir une gouvernance éthique dans un contexte d'incertitudes croissantes.

3.2 Objectif du contrôle interne :

L'objectif général du contrôle interne est de garantir la continuité de l'entreprise dans la réalisation de ses buts et de ses stratégies (Henk, 2020). Pour atteindre cet objectif, le dispositif de contrôle interne se décline en quatre rubriques interdépendantes.

3.2.1. La Protection du Patrimoine

Un bon système de contrôle interne se doit avant tout de sauvegarder les actifs de l'entreprise, aussi désigné sous l'appellation « sécurité des actifs ». En effet, le patrimoine de l'entreprise – englobant l'ensemble des différents postes du bilan – demeure vulnérable aux risques d'erreurs,

aux mauvaises décisions, mais aussi aux vols ou fraudes. Ainsi, selon Renard (2012), un contrôle rigoureux est indispensable pour préserver ces ressources vitales.

3.2.2. La Fiabilité et l'Intégrité des Informations Financières et Opérationnelles

Cet objectif est souvent privilégié, car il met en lumière la nécessité d'organiser les fonctions comptables et financières de manière à garantir la qualité et la véracité des informations produites. Cette garantie permet aux gestionnaires et autres parties prenantes de prendre des décisions éclairées. Pour ce faire, le contrôle interne s'appuie sur quatre principes fondamentaux :

- **La fiabilité :** Le système doit être en mesure de fournir des preuves attestant de la vérification et de l'exactitude des informations financières.
- **La pertinence :** L'information doit être adaptée aux besoins des utilisateurs des états financiers, facilitant ainsi des prises de décisions appropriées.
- **La disponibilité :** Les informations doivent être facilement accessibles et fournies en temps utile.
- **L'exhaustivité :** Au-delà de l'exactitude, il est essentiel que l'information soit complète, couvrant l'ensemble des enregistrements nécessaires à une représentation fidèle de la réalité financière.

3.2.3. Le Respect des Instructions de la Direction et la Conformité aux Lois et Réglementations

Pour assurer une gouvernance efficace, le contrôle interne doit garantir le strict respect des directives données par la direction, lesquelles s'expriment sous diverses formes (automatisées, écrites ou verbales) et peuvent revêtir un caractère permanent, temporaire ou ponctuel. En parallèle, il est impératif que l'entreprise se conforme à l'ensemble des lois et réglementations applicables, couvrant des domaines tels que la fiscalité, le droit du travail, le droit des sociétés, le droit commercial, la sécurité ou encore l'environnement.

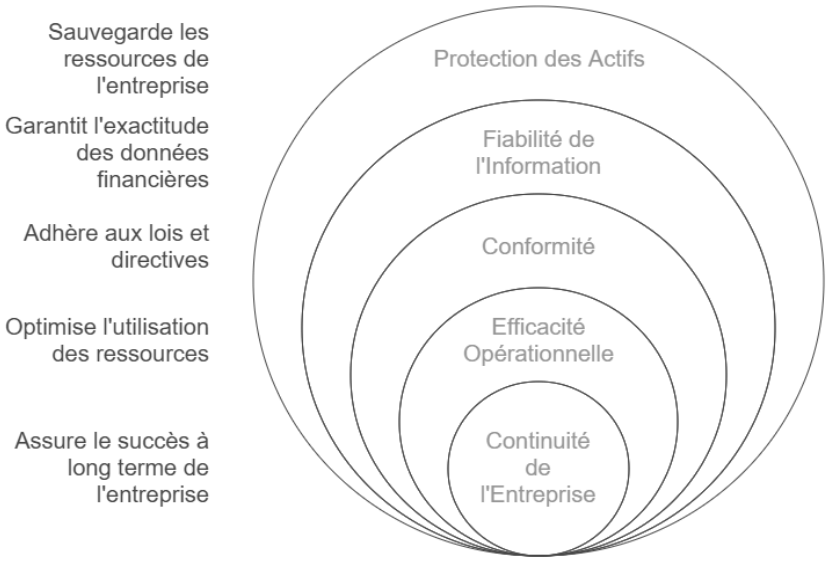
3.2.4. L'Efficacité et l'Efficience des Opérations

Également désigné sous l'appellation de « maîtrise de l'entreprise », cet objectif vise à optimiser l'utilisation des ressources internes afin d'atteindre les objectifs stratégiques fixés. En

améliorant l'efficience opérationnelle, le contrôle interne contribue à la compétitivité et à la pérennité de l'organisation, en veillant à ce que chaque ressource soit utilisée de manière optimale.

Afin de mieux comprendre l'organisation de ces objectifs, ils sont souvent présentés sous forme de matrice,

Figure 5 : Matrice récapitulative des objectifs du contrôle interne



Source : (Henk, 2020)

Les objectifs généraux du contrôle interne convergent vers une vision commune :

Protéger les actifs, garantir la fiabilité des informations, prévenir les risques et assurer la conformité légale et opérationnelle. Cependant, les spécificités des référentiels permettent de répondre à des besoins variés et adaptés à chaque secteur ou contexte. COSO et ISO 31000 offrent une approche holistique et intégrée, tandis que COBIT cible les enjeux technologiques, et le Comité de Bâle et SOX répondent à des impératifs financiers et réglementaires spécifiques. La diversité de ces cadres permet aux entreprises de choisir, ou de combiner, des approches pour structurer un contrôle interne efficace et stratégique, favorisant leur performance et leur pérennité dans un environnement mondial complexe.

Chaque référentiel international apporte une perspective unique sur le contrôle interne en fonction des contextes sectoriels, géographiques ou techniques qu'il adresse. Voici un aperçu des spécificités clés :

COSO : Garantir l'efficacité des opérations, la fiabilité financière et la conformité réglementaire dans une approche holistique.

COCO : Mettre l'accent sur la culture éthique et la responsabilité individuelle au sein de l'organisation.

ISO 31000 : Anticiper les incertitudes et gérer les risques de manière proactive pour renforcer la prise de décision.

COBIT : Sécuriser les données critiques et aligner les systèmes IT avec les objectifs stratégiques.

Comité de Bâle : Assurer la transparence et gérer les risques financiers spécifiques au secteur bancaire.

SOX : Prévenir les fraudes comptables et garantir la confiance des investisseurs grâce à des processus rigoureux.

3.3. Méthodologie et outils du contrôle interne :

Un contrôle interne efficace repose sur des méthodologies structurées et des outils adaptés qui permettent d'assurer la réalisation des objectifs stratégiques, de protéger les actifs et de prévenir les risques. Ce dispositif nécessite une approche globale, combinant des référentiels reconnus, des outils pratiques et une implication constante des acteurs internes (Hoai, and Nguyen, 2022).

4.1 l'utilisation de référentiels reconnus :

Les référentiels internationaux tels que COSO, souvent cités comme les cadres de référence, fournissent une base méthodologique incontournable. Ils permettent de structurer le contrôle interne en assurant une cohérence entre les processus.

Le modèle COSO (un exemple clé): COSO, utilisé dans le monde entier, définit cinq composantes interdépendantes (Carassus and Cormier, 2003) :

Il définit cinq composantes interdépendantes nécessaires à un système de contrôle interne robuste :

a. l'environnement de contrôle, c'est-à-dire la culture de l'organisation, l'éthique, la structure de gouvernance et l'implication de la direction (un ton managérial favorable au contrôle, des responsabilités clairement définies, des procédures formalisées) ;

b. l'évaluation des risques, par l'identification systématique et l'analyse des risques susceptibles d'affecter l'atteinte des objectifs, puis la hiérarchisation de ces risques en fonction de leur impact et de leur probabilité ;

c. les activités de contrôle, qui regroupent l'ensemble des mesures de maîtrise mises en place pour atténuer les risques identifiés il peut s'agir de politiques, de procédures, de vérifications, d'autorisations, de séparations de tâches, etc., proportionnées aux enjeux et intégrées aux processus de l'organisation ;

d. L'information et la communication, visant à garantir que les informations pertinentes (comptables, financières ou opérationnelles) soient collectées, traitées de manière fiable et diffusées aux bonnes personnes en temps utile, et qu'il existe des canaux de communication efficaces tant en interne (sensibilisation des employés au dispositif de contrôle) qu'en externe (reporting aux parties prenantes) ;

e. le pilotage et la surveillance du dispositif de contrôle interne, qui impliquent un suivi continu et des évaluations régulières de l'efficacité des contrôles en place. Ce dernier aspect inclut les auto-évaluations par les responsables opérationnels eux-mêmes, mais aussi des évaluations indépendantes, notamment par la fonction d'audit interne. L'audit interne est en effet chargé de vérifier périodiquement que le système de contrôle fonctionne correctement et d'en signaler les faiblesses, contribuant ainsi à son amélioration continue.

4.2 Les outils du contrôle interne :

Les outils sont indispensables pour traduire les principes méthodologiques en actions concrètes (O'Leary, Iselin, and Sharma, 2006) :

- **La cartographie des risques:** un outil clé qui permet de:

  - Consiste à recenser et représenter les risques majeurs de l'organisation (financiers, opérationnels, juridiques, etc.)
  - Vérifier que des contrôles appropriés sont en place pour chaque risque.
  - Prioriser les actions de contrôle interne en fonction du niveau de risque.

Certains logiciels sp6écialisés comme Audit Board ou Resolver permettent une cartographie dynamique avec mise à jour automatique en fonction des données nouvelles.

- **Le manuel de procédures et les politiques internes :** qui documentent de façon formelle les contrôles à effectuer, les rôles et responsabilités attribués à chacun, servent de référence aux employés.

Technologies modernes :

- Les ERP (ex. SAP) ou les logiciels GRC (Governance, Risk and Compliance) offrent une automatisation des contrôles et des analyses en continu.
- Enrichissement : L'utilisation de l'IA et du machine learning dans ces logiciels peut détecter des anomalies, comme des transactions inhabituellement élevées.

Indicateurs de performance et tableaux de bord :

- Ils permettent de mesurer l'efficacité des contrôles en place et de surveiller les écarts en temps réel.
- Exemple : Suivi des retards dans le traitement des factures pour détecter un potentiel dysfonctionnement.

4.3 L'audit interne : un acteur central

L'audit interne et le contrôle interne jouent un rôle significatif dans la prévention de la fraude, contribuant ensemble à hauteur de 68,8 % à la réduction du risque. (Universitas Widyatama *et al.*, 2020)

C'est le garant de l'efficacité du contrôle interne et joue un rôle critique dans son amélioration continue.

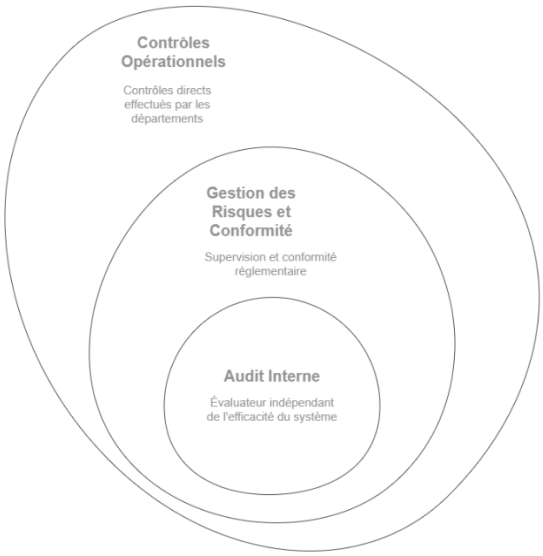
Le modèle de trois lignes de défense: la mise en œuvre du contrôle interne s'appuie souvent sur le principe des « trois lignes de défense » (Bantleon et al,2020) :

- **Première ligne** : Les contrôles opérationnels sont effectués directement par les services concernés, tels que la vérification des rapprochements bancaires par le service financier.
- **Deuxième ligne** : Les fonctions de gestion des risques et de conformité, qui supervisent les activités et vérifient que les processus respectent les exigences réglementaires.

- **Troisième ligne** : L'audit interne, qui agit comme un évaluateur indépendant pour garantir que le système global est efficace et fonctionne selon les meilleures pratiques.

Voici un schéma récapitulatif des modèles des 3 lignes de défenses :

Figure 6 : Contrôles opérationnels et conformité réglementaire



Source : (Bantleon et al,2020)

L'impact stratégique de l'audit interne :

L'audit interne ne se limite pas à identifier des faiblesses ; il agit également comme un conseiller stratégique auprès de la direction, proposant des solutions d'amélioration concrètes. Il contribue activement à la prévention des fraudes par des enquêtes ciblées et assure la conformité des pratiques en surveillant de près les évolutions législatives et normatives. Enrichissement : Grâce aux innovations en analyse de données (data analytics), l'audit interne peut désormais analyser rapidement des millions de transactions pour détecter efficacement les écarts et anomalies (Roussy, and Perron, 2018).

La mise en place d'un contrôle interne robuste repose sur un cadre méthodologique cohérent, appuyé par des outils efficaces et des acteurs centraux comme l'audit interne. Les référentiels reconnus offrent des bases solides qui peuvent être enrichies par des technologies modernes et des approches proactives. L'utilisation de la cartographie des risques, des tableaux de bord et

des logiciels GRC permet une gestion dynamique et adaptée aux évolutions de l'environnement. En s'appuyant sur le modèle des trois lignes de défense, les organisations peuvent garantir une maîtrise intégrale des risques, tout en alignant leurs pratiques sur les normes internationales. Ce dispositif est essentiel pour favoriser la résilience, la performance et la pérennité des entreprises.

4.4. Limites du contrôle interne

La mise en œuvre du contrôle interne est une pratique fondamentale dans la gouvernance des organisations modernes. Cependant, cette démarche, bien qu'indispensable, n'est pas exempte de limites qui peuvent impacter son efficacité et sa pertinence. L'objectif de ce travail est de synthétiser les contraintes inhérentes au contrôle interne, tout en soulignant les enjeux liés à son amélioration continue.

- **Dépendance à la culture organisationnelle**

Le contrôle interne est intrinsèquement lié à la culture éthique et aux valeurs portées par l'organisation. La qualité de l'environnement de contrôle, tel que défini par le référentiel COSO, repose sur l'engagement de la direction à promouvoir un cadre éthique robuste et une gouvernance exemplaire (Henk, 2020) . En l'absence de cette dynamique, même des procédures élaborées peuvent être inefficaces. Ainsi, la culture organisationnelle constitue un levier mais également une vulnérabilité, car elle dépend de la cohérence des comportements individuels et collectifs.

- **Formalisation excessive des processus**

Bien que la définition de procédures claires et détaillées soit essentielle, un excès de formalisation peut nuire à la flexibilité opérationnelle, notamment dans des environnements dynamiques où les risques évoluent rapidement. En s'appuyant sur des cadres comme ISO 31000, il est évident que l'adaptabilité constitue un élément clé de la gestion des risques. Un dispositif trop rigide peut ainsi limiter la capacité de l'organisation à intégrer des menaces émergentes, telles que les cyberattaques ou les changements réglementaires.

- **Lacunes dans l'évaluation des risques**

Une autre limite concerne l'évaluation des risques. Bien que la cartographie des risques soit un outil clé dans la méthodologie du contrôle interne, son efficacité repose sur sa mise à jour régulière. Les référentiels comme COSO ou ISO 31000 encouragent une approche proactive,

mais en pratique, les organisations peuvent négliger certains risques nouveaux, notamment ceux liés aux innovations technologiques ou aux contextes géopolitiques fluctuants.

- **Dépendance aux outils technologiques**

Les avancées technologiques, notamment l'automatisation par les systèmes ERP ou les logiciels de GRC, ont permis d'optimiser les processus de contrôle. Toutefois, ces outils présentent leurs propres limites, tels que la vulnérabilité aux cyberattaques ou la nécessité d'une maintenance constante. COBIT souligne l'importance de gouverner ces systèmes, mais une dépendance excessive aux technologies peut conduire à des dysfonctionnements non détectés, compromettant l'intégrité des contrôles.

- **Contraintes liées à l'audit interne**

L'audit interne, bien qu'il joue un rôle crucial dans le contrôle interne, peut être limité par un manque de ressources humaines, financières ou d'indépendance. Conformément au modèle des trois lignes de défense, l'audit interne doit garantir l'efficacité des contrôles. Cependant, si les premières lignes (opérationnelle et fonctionnelle) ne fonctionnent pas de manière optimale, la charge sur l'audit interne peut devenir disproportionnée, réduisant son efficacité.

- **Coûts élevés de mise en œuvre**

La mise en œuvre d'un contrôle interne conforme aux normes internationales peut entraîner des coûts significatifs, notamment pour les petites et moyennes entreprises. Par exemple, des réglementations telles que la loi Sarbanes-Oxley exigent des audits approfondis et des dispositifs robustes, parfois inaccessibles pour les organisations aux ressources limitées.

- **Risques liés au facteur humain**

Enfin, le facteur humain reste une limite majeure du contrôle interne. Des erreurs, des négligences ou des comportements malveillants peuvent compromettre l'efficacité des dispositifs, malgré la formalisation des contrôles et des processus. Les référentiels comme COCO mettent en lumière la nécessité de sensibiliser les employés à l'importance des contrôles, mais ces actions ne peuvent totalement prévenir les défaillances humaines.

En conclusion, le contrôle interne, bien qu'essentiel pour la gouvernance et la gestion des risques, est soumis à des contraintes organisationnelles, technologiques, humaines et financières. Ces limites soulignent l'importance d'une démarche d'amélioration continue et d'une intégration intelligente des technologies. Les organisations doivent adopter une approche

équilibrée entre flexibilité et rigueur, tout en renforçant leur culture éthique et leur capacité d'adaptation face aux risques émergents. En s'appuyant sur les référentiels reconnus et les meilleures pratiques, elles peuvent surmonter ces défis et garantir la pérennité et la résilience de leur dispositif de contrôle interne.

CHAPITRE II : Contexte organisationnel de l'entreprise étudié

Introduction :

Le chapitre suivant décrit le contexte organisationnel de l'entreprise étudiée, en utilisant des données provenant de divers documents internes et d'informations recueillies auprès des responsables de l'entreprise. Il comprend également un cadre méthodologique qui inclut des études à la fois qualitatives et quantitatives, ainsi que des informations sur les procédures de la recherche et une approche épistémologique.

Ce chapitre se divise en deux sections principales. La première section présente une analyse détaillée du contexte organisationnel de l'entreprise, en mettant en lumière son historique, sa structure de gouvernance, ses domaines d'activité, et ses stratégies de contrôle interne. Cette analyse permet de comprendre les fondements et les dynamiques internes de l'entreprise, ainsi que les défis et opportunités auxquels elle est confrontée en matière de contrôle interne.

La deuxième section expose le cadre méthodologique de l'étude, en détaillant les approches qualitatives et quantitatives adoptées pour explorer le rôle du contrôle interne dans la prévention et la détection de la fraude. Cette section inclut une description des méthodes de collecte et d'analyse des données, ainsi que des procédures de recherche et de l'approche épistémologique sous-jacente. Elle vise à fournir une base solide pour l'interprétation des résultats et la formulation de recommandations pertinentes.

En combinant ces deux sections, ce chapitre offre une vue d'ensemble complète et intégrée du contexte organisationnel de l'entreprise et des méthodes utilisées pour mener cette étude. Il prépare ainsi le terrain pour une analyse approfondie des mécanismes de contrôle interne et de leur efficacité dans la prévention et la détection de la fraude.

Section 1 : Présentation de PwC

PricewaterhouseCoopers International Limited (PwC) est un réseau mondial de cabinets offrant des services en audit, expertise, conseil financier, comptable, juridique et gestion d'entreprise. PwC fait partie des Big Four aux côtés de KPMG, EY et Deloitte. En 2018, PwC était le deuxième plus grand cabinet en termes de chiffre d'affaires parmi les Big Four, avec 41,3 milliards de dollars. PwC est une marque sous laquelle les sociétés membres de PwC opèrent.

PwC coordonne les activités des entités membres du réseau PwC, qui sont juridiquement autonomes et présentes dans 158 pays avec plus de 250 000 collaborateurs.

2.1 Historique de PwC

PricewaterhouseCoopers (PwC) est le résultat de la fusion en 1998 de deux cabinets comptables historiques : Price Waterhouse et Coopers & Lybrand. Voici les étapes clés de son évolution :

1849 : Samuel Lowell Price fonde son cabinet à Londres.

1854 : William Cooper crée son propre cabinet, qui deviendra plus tard Cooper Brothers.

1865 : Edwin Waterhouse rejoint le cabinet de Price, qui devient Price Waterhouse.

1957 : Coopers & Lybrand International est créé par l'association de Cooper Brothers & Co (Royaume-Uni), Lybrand, Ross Bros & Montgomery (États-Unis) et McDonald, Currie & Co (Canada).

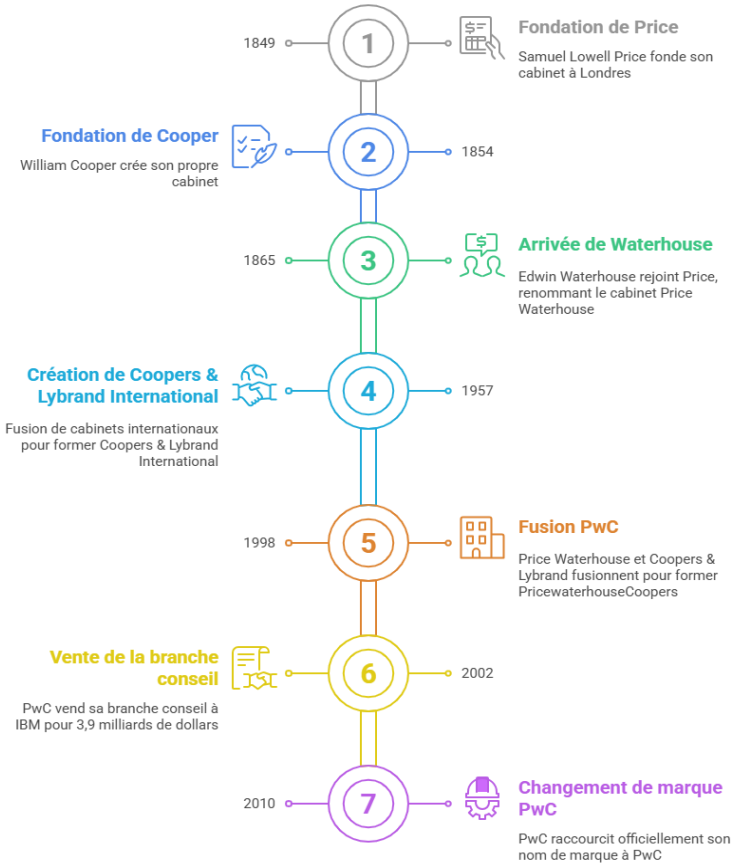
1998 : Fusion de Price Waterhouse et Coopers & Lybrand pour former PricewaterhouseCoopers.

2002 : PwC vend sa branche conseil à IBM pour 3,9 milliards de dollars.

2010 : PwC raccourcit officiellement son nom de marque à PwC, tout en conservant légalement le nom PricewaterhouseCoopers.

Aujourd'hui, PwC est l'un des plus grands réseaux de services professionnels au monde, avec une présence dans 158 pays et plus de 250 000 collaborateurs.

Figure 7 : L'évolution historique de PwC : des origines à la marque actuelle.



Source : Document Interne document interne Pwc.

La figure retrace les étapes clés de la formation et du développement de PwC, depuis la création des cabinets fondateurs jusqu'à l'adoption de son nom actuel, en passant par des fusions et des changements stratégiques.

2.2 PwC Algérie

PwC Algérie est une branche du réseau mondial PwC, spécialisée dans les services d'audit, de conseil, d'expertise juridique et fiscale. Le bureau d'Alger, qui compte environ 100 collaborateurs, se distingue par sa réactivité et sa proximité avec les clients.

2.3 Historique et Présence

PwC Algérie fait partie intégrante du réseau PwC, qui est présent dans 158 pays et emploie plus de 250 000 personnes à travers le monde. Le réseau PwC a été formé en 1998 suite à la fusion de Price Waterhouse et Coopers & Lybrand, deux cabinets comptables historiques. Price

Waterhouse a été fondé en 1849 par Samuel Lowell Price à Londres, tandis que Coopers & Lybrand trouve ses origines en 1854 avec la création du cabinet de William Cooper. En 1957, Coopers & Lybrand International a été créé par l'association de plusieurs cabinets, dont Cooper Brothers & Co (Royaume-Uni), Lybrand, Ross Bros & Montgomery (États-Unis) et McDonald, Currie & Co (Canada). La fusion de 1998 a permis de créer l'entité actuelle, PricewaterhouseCoopers, qui a ensuite raccourci son nom de marque à PwC en 2010 tout en conservant légalement le nom complet.

2.4 Services et Expertises

PwC Algérie offre une gamme complète de services professionnels, notamment :

Audit : Les services d'audit de PwC Algérie incluent la vérification des états financiers et l'assurance de la conformité aux normes comptables internationales. Les audits sont réalisés avec une rigueur méthodologique pour garantir la fiabilité des informations financières des entreprises.

Conseil : PwC Algérie accompagne les entreprises dans leur transformation stratégique et opérationnelle. Les services de conseil couvrent des domaines tels que la gestion des risques, l'amélioration des processus, la transformation digitale et la stratégie de croissance.

Expertise juridique et fiscale : Les experts de PwC Algérie fournissent des conseils en matière de droit des affaires, de fiscalité et de conformité réglementaire. Ils aident les entreprises à naviguer dans les complexités juridiques et fiscales pour optimiser leur performance et minimiser les risques.

2.5 Distinctions et Engagements

PwC Algérie a été certifié Top Employer 2025, une reconnaissance de l'excellence de ses politiques de ressources humaines. Cette certification met en avant les efforts de PwC Algérie en matière d'intégration des nouveaux employés, de gestion de carrière, de politique de rémunération et de promotion de la diversité. Le bureau d'Alger est également engagé dans des initiatives visant à renforcer l'équité professionnelle et à lutter contre la fraude. Ces engagements se traduisent par des programmes de formation continue, des actions de sensibilisation et des partenariats avec des organisations locales et internationales.

Initiatives et Projets

Le bureau d'Alger participe activement à des projets visant à soutenir le développement économique et social en Algérie. Cela inclut des collaborations avec des organisations locales et internationales pour promouvoir la transparence, l'innovation et la croissance durable. PwC Algérie s'implique également dans des initiatives de responsabilité sociale, telles que des programmes de mentorat pour les jeunes entrepreneurs, des actions de soutien aux communautés locales et des projets environnementaux visant à réduire l'empreinte carbone des entreprises.

Assurance & Audit LoS

Le stage que j'ai effectué chez PwC Algérie s'est déroulé dans le département Assurance & Audit, dirigé par deux directeurs d'audit et composé d'une centaine d'auditeurs de différents grades, allant des Auditeurs Juniors aux Senior Managers. Les principales missions de ce département incluent le commissariat aux comptes et l'audit contractuel. Pour ces missions, PwC Algérie utilise divers outils informatiques qui facilitent les travaux des auditeurs :

Communication sécurisée : Utilisation de trois logiciels de messagerie et de communication pour des échanges sécurisés avec les clients et les bureaux PwC à l'étranger.

Maintenance informatique : Service de maintenance à distance disponible 24h/24 pour résoudre les problèmes logiciels rencontrés par les auditeurs.

Logiciel d'audit interne : Un logiciel développé en interne qui couvre l'ensemble des travaux d'audit, de l'acceptation de la mission à l'émission du rapport d'audit. Ce logiciel, conçu pour documenter les travaux d'audit de manière simple et organisée, propose des modèles de travail conformes aux réglementations IAS/IFRS et locales, avec des guidances et des renvois aux textes de loi et normes d'audit appropriés.

Portail Intranet : Contient des informations sur le réseau PwC, des faits d'actualité et des formations en e-Learning, mis à jour avec l'évolution des normes internationales de comptabilité et d'audit.

Documentation électronique : Inclut les normes de comptabilité, d'audit et de gestion des risques, ainsi que des documents internes propres à la politique et à la méthodologie PwC.

Les missions d'audit chez PwC Algérie sont réalisées selon une méthodologie spécifique et standardisée à l'ensemble des entreprises du réseau PwC, appelée PwC Audit Policy. Cette

méthodologie, conçue selon l'approche d'audit par les risques, vise à encadrer les travaux des auditeurs.

Section 2 : Etude de cas démarche méthodologique

L'étude de cas constitue une stratégie pertinente lorsqu'on cherche à comprendre un phénomène complexe dans son contexte réel. Nous avons souhaité explorer en profondeur les pratiques internes de prévention et de détection de la fraude, telles qu'elles sont mises en œuvre dans une organisation reconnue pour ses standards élevés en matière d'audit et de contrôle interne. Le cas de fraude qui constitue le cœur de cette étude a été détecté au sein d'une agence d'assurance dans l'Ouest algérien. Il s'agit d'un cas réel, traité de manière strictement anonyme, et documenté à partir de plusieurs sources : entretiens semi-directifs, rapport d'audit interne, relevés comptables, et compte rendu de la commission de discipline.

2.1 Nature de l'approche méthodologique :

Notre étude s'inscrit dans une approche qualitative de type interprétatif, fondée sur une étude de cas approfondie. Elle vise à produire une compréhension fine des représentations, des pratiques et des perceptions des professionnels face aux enjeux de la fraude et aux dispositifs de contrôle interne. Ce type de recherche permet de faire émerger des connaissances contextualisées, construites à partir des discours et des expériences des acteurs directement impliqués dans le terrain étudié.

2.2. Épistémologie et paradigmes de recherche :

L'épistémologie est la branche de la philosophie qui étudie la nature, les sources et la validité de la connaissance (Piaget, 1967). Elle s'intéresse aux questions fondamentales telles que : Qu'est-ce que la connaissance ? Comment est-elle acquise ? Qu'est-ce qui distingue une croyance justifiée d'une opinion ? En recherche, l'épistémologie influence fortement le choix des méthodes car elle détermine ce qui est considéré comme une preuve acceptable et valide (Avenier & Thomas, 2015).

2.3. Le Paradigme constructiviste :

Le paradigme constructiviste repose sur l'idée que la réalité est construite socialement par les acteurs. Il met l'accent sur la compréhension en profondeur des phénomènes sociaux à travers l'interprétation des expériences vécues par les individus (Lee, 2011). Dans le cadre de cette recherche, ce paradigme s'est révélé pertinent pour explorer les perceptions subjectives des

professionnels interrogés sur le contrôle interne et la fraude. Car Dans cette optique, il ne s'agit pas de découvrir une vérité objective mais de comprendre comment les acteurs donnent sens à leur environnement et à leurs pratiques. En adoptant cette perspective, l'étude s'ancre dans une logique interprétative qui valorise les récits, les discours et les significations attribuées par les acteurs à leurs pratiques quotidiennes.

2.4 Outils de collecte des données :

Dans cette partie, nous allons examiner les méthodes de collecte de données qualitatives utilisées dans notre étude. Ces méthodes incluent l'observation, l'analyse documentaire et les entretiens.

A. L'observation

L'observation est une technique essentielle en recherche qualitative pour recueillir des données sur le terrain. Elle consiste à observer et enregistrer les comportements, les interactions et les phénomènes dans leur contexte naturel, sans intervenir ou perturber la situation. Il existe deux formes d'observation :

- **Observation directe** : Le chercheur est physiquement présent sur le terrain pour observer les événements en temps réel.
- **Observation indirecte** : L'observation est réalisée à partir d'enregistrements audio, vidéo ou écrits.

B. L'Analyse documentaire

Cette méthode implique l'examen des documents internes et externes d'une organisation, tels que les fichiers PDF, les normes, les rapports et les politiques. L'objectif est d'extraire des informations pertinentes pour la recherche, ce qui permet d'accentuer l'objectivité et la rigueur de l'étude.

C. Les entretiens

Les entretiens sont un outil majeur de collecte de données en recherche qualitative, car ils permettent d'explorer en profondeur les expériences, opinions et perceptions des participants. On distingue trois types d'entretiens :

- **Entretiens directifs** : Suivent un questionnaire avec des questions précises à réponses fermées.
- **Entretiens non-directifs** : Très ouverts, laissant les participants aborder librement les sujets.
- **Entretiens semi-directifs** : Combinent un canevas de questions avec une certaine flexibilité pour approfondir certains points.

Dans notre étude, nous avons opté pour des entretiens semi-directifs individuels auprès de dirigeants et de managers (6 cadres), en suivant un guide d'entretien structuré par thèmes. Le guide d'entretien a pour objectif de fournir un cadre général, tout en étant flexible aux réponses et aux questions. Les entretiens, d'une durée d'environ 45 minutes, ont été enregistrés avec l'accord des participants.

2.5 Échantillonnage qualitatif :

L'échantillonnage qualitatif vise à sélectionner des participants qui peuvent fournir des informations riches et pertinentes sur les pratiques de contrôle interne et la prévention de la fraude au sein de l'entreprise. L'objectif est de recueillir des données détaillées et variées pour obtenir une compréhension approfondie du phénomène étudié.

2.6 Analyse des données :

Pour analyser les données qualitatives issues des entretiens, nous avons choisi la méthode d'analyse thématique, adaptée pour examiner des perspectives multiples (Fourar, 2023). (Poth et Creswell ,2018, p.232) la définissent ainsi :

"L'analyse thématique vise à trouver, analyser et interpréter les modèles ou thèmes récurrents dans un ensemble de données. Son principal objectif est de bien comprendre les données et d'identifier les hypothèses, significations ou interprétations sous-jacentes."

Nous suivons un processus itératif et systématique de codage, de catégorisation thématique, de mise en relation des thèmes et d'interprétation approfondie, comme décrit par (Fouial, 2023). Cette approche rigoureuse implique le suivi des étapes suivantes :

D. **Collecte et organisation des données brutes** :

Cette étape consiste à rassembler toutes les données qualitatives recueillies, telles que les transcriptions des entretiens, les notes de terrain, et les documents pertinents. Les données sont ensuite organisées de manière systématique pour faciliter l'analyse.

E. **Codage initial du corpus en unités de sens** :

Le codage initial implique de diviser les données en unités de sens, c'est-à-dire en segments de texte qui représentent des idées ou des concepts distincts. Chaque unité de sens est ensuite attribuée à un code descriptif.

F. **Recherche de thèmes émergents par analyse des codes connexes** :

Une fois les données codées, nous analysons les codes pour identifier des thèmes émergents. Les thèmes sont des catégories plus larges qui regroupent des codes connexes et représentent des motifs récurrents dans les données.

G. **Révision et raffinement des thèmes** :

Les thèmes identifiés sont ensuite révisés et affinés pour s'assurer qu'ils sont cohérents et représentatifs des données. Cette étape peut impliquer la fusion de thèmes similaires, la division de thèmes trop larges, ou la réévaluation de certains codes.

H. **Définition et dénomination précise des thèmes** :

Chaque thème est défini de manière précise et nommé de façon à refléter son contenu. Cette étape permet de clarifier les significations des thèmes et de faciliter leur interprétation.

. Une première lecture a permis de construire une grille de codage thématique. Ensuite, les occurrences ont été regroupées en nœuds permettant d'identifier des tendances, des convergences et des tensions entre les discours. Cette analyse a également permis de faire émerger des dimensions transversales telles que la culture organisationnelle, la pression réglementaire ou l'influence des outils numériques.

A. Méthode

Nous utiliserons un échantillonnage intentionnel, également appelé échantillonnage par choix raisonné. Cette méthode consiste à sélectionner des participants en fonction de critères spécifiques, tels que leur rôle, leur expérience, et leur connaissance des pratiques de contrôle interne. L'échantillonnage intentionnel permet de cibler des informateurs clés qui peuvent fournir des insights précieux sur le sujet.

B. Critères de sélection

Les critères de sélection des participants incluent :

- **Rôle dans l'entreprise** : Responsables du contrôle interne, auditeurs internes, managers financiers, chefs de service.
- **Expérience** : Participants ayant une expérience significative dans la mise en œuvre et la gestion des pratiques de contrôle interne.
- **Connaissance des pratiques de contrôle interne** : Participants ayant une connaissance approfondie des mécanismes de contrôle et des stratégies de prévention de la fraude.

C. Taille de l'échantillon :

L'échantillon sera composé de 6 participants. Cette taille est suffisante pour obtenir une diversité de perspectives et atteindre la saturation théorique. La saturation théorique est atteinte lorsque les nouvelles données n'apportent plus d'informations supplémentaires significatives.

D. Processus de sélection :

Le processus de sélection des participants comprend les étapes suivantes :

1. **Identification des rôles clés** : Identifier les rôles clés au sein de l'entreprise qui sont directement impliqués dans les pratiques de contrôle interne.
2. **Évaluation de l'expérience et des connaissances** : Évaluer l'expérience et les connaissances des candidats potentiels en matière de contrôle interne et de prévention de la fraude.
3. **Sélection des participants** : Sélectionner les participants en fonction des critères de rôle, d'expérience et de connaissance.

Tableau des personnes interviewées :

Voici un tableau récapitulatif des personnes interviewées :

Statut Hiérarchique	**Ancienneté**	**Type d'Entretien**	**Durée de l'Entretien**
Directeur d'Agence	10 ans	Face à face individuel	25 min
Chef de service comptabilité (Direction régionale)	13 ans	Face à face individuel	25 min
Chef de service comptabilité (direction régionale)	12 ans	Face à face individuel	25 min
Directeur Central des Systèmes d'Information	11 ans	Face à face individuel	30 min
Directeur régionale	25 ans	Face à face individuel	30 min
Directeur central des risques de masse et des particuliers	16 ans	Face à face individuel	25 min

Tableau 2 : Tableau récapitulatif des personnes interviewées

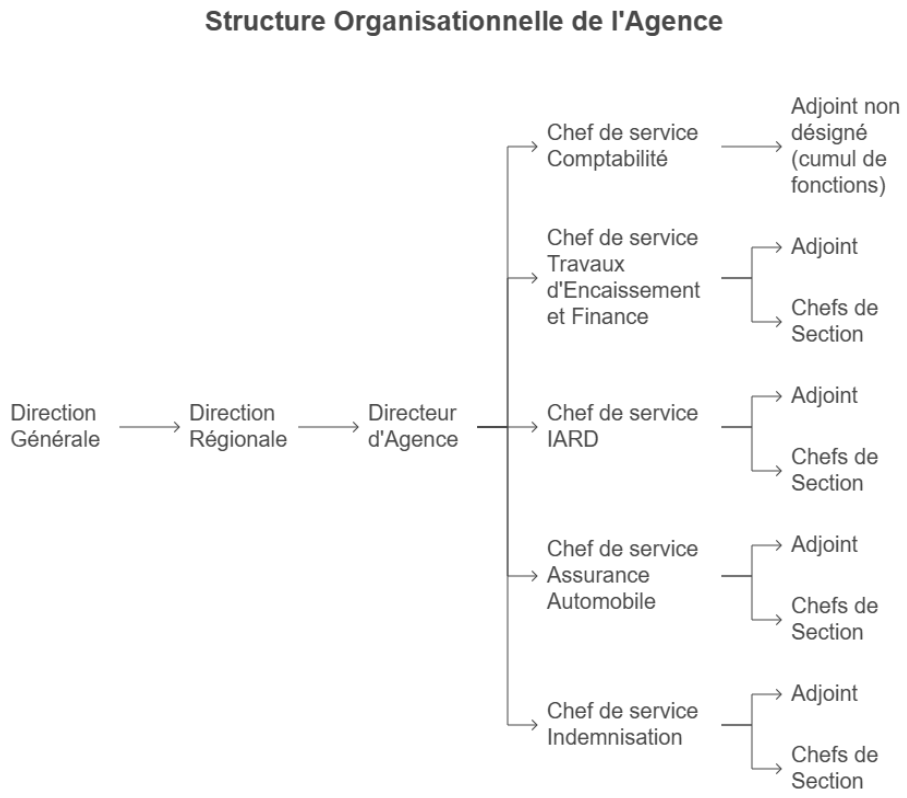
L'échantillonnage qualitatif permet de sélectionner des participants qui peuvent fournir des informations riches et pertinentes sur les pratiques de contrôle interne et la prévention de la fraude. En utilisant un échantillonnage intentionnel, nous pouvons cibler des informateurs clés et obtenir une diversité de perspectives pour une compréhension approfondie du phénomène étudié.

Section 3 : Contexte et déroulement des faits

Les faits concernent un agent occupant des responsabilités comptables au sein de l'agence. Ce dernier a exploité une série de failles organisationnelles et informatiques pour procéder à des **manipulations frauduleuses de paiements**. Le mode opératoire consistait à **supprimer des polices d'assurance réglées par chèque** (essentiellement des contrats de la branche IARD), afin de réaffecter les montants de ces chèques à d'autres polices souscrites en espèces, notamment dans la branche automobile.

Par cette substitution, l'agent annulait l'avis de versement en espèces, détournait les fonds encaissés physiquement, et affectait à la place un chèque ~~déjà encaissé et~~ rattaché à une police supprimée. Cette pratique permettait de **donner une apparente cohérence comptable** aux états de fin de journée, en masquant les écarts d'encaissement. Le comptable passait des écritures d'encaissements des polices auto par le chèque initialement destin » à payer le contrat d'assurance IARD.

Le diagramme ci-dessus va nous permettre de mieux comprendre l'organisation de l'agence



Source : Document interne de l'entreprise

3.3.2 Mécanisme et exploitation des failles

Plusieurs facteurs ont permis à l'agent d'agir sans détection immédiate :

- **Le cumul des fonctions** : la même personne assurait à la fois l'encaissement et la comptabilisation des primes, en contradiction avec les principe de séparation des tâches.

- **L'accès non sécurisé au système ERP** : l'agent a utilisé la session d'un collègue chargé de la sousciption de polces d'assurance restée ouverte pour effectuer des opérations de suppression non autorisées.
- **L'absence de contrôle spécifique sur les suppressions de polices et d'avis de versement**, aucun mécanisme d'alerte n'étant mis en place.
- **L'insuffisance des rapprochements entre états de production technique et comptabilité**.

Ces failles ont été confirmées lors de la mission d'inspection menée par les services centraux, à l'issue de laquelle un rapport a été établi.

3.3.3 Détection et suites disciplinaires

La fraude a été découverte de manière fortuite par le directeur d'agence, qui, en manipulant des documents physiques, a constaté la présence de **polices supprimées dans le système mais toujours existantes en version papier**, accompagnées de chèques de règlement. Après avoir interrogé l'agent mis en cause sans obtenir d'explication convaincante, une mission d'audit a été diligentée. Ce chèque relatif au paiement d'une police supprimée devait servir à payer des polices auto encaissées en espèces.

Lors de la réunion de la commission de discipline, **l'agent a reconnu les faits dans leur intégralité**. Il a présenté ses excuses et sollicité un délai pour rembourser le préjudice. Toutefois, compte tenu de la gravité des faits, la commission a prononcé son **licenciement immédiat et sans préavis**. Le rapport de l'inspecteur chargé a souligné les défaillances du contrôle interne, notamment celles liées à la gestion des habilitations et à la sécurité des sessions informatiques.

Conclusion du chapitre

Ce chapitre a permis d'exposer de manière structurée le cadre méthodologique retenu pour cette recherche, ainsi que le contexte organisationnel dans lequel elle s'inscrit. L'étude repose principalement sur une **approche qualitative**, centrée sur un **cas réel de fraude interne** survenu dans une agence d'assurance, analysé à travers des **entretiens semi-directifs** menés avec différents acteurs à tous les niveaux hiérarchiques de l'organisation.

La présentation détaillée du **cas de fraude** a permis d'illustrer concrètement les vulnérabilités du dispositif de contrôle interne en place, en mettant en évidence les failles procédurales, les

dysfonctionnements organisationnels et les lacunes en matière de sécurité des systèmes d'information. Ce cas constitue un levier central pour comprendre les mécanismes de contournement des contrôles et les facteurs humains et techniques favorisant la fraude.

La **démarche méthodologique** repose sur une **analyse thématique** rigoureuse, menée à l'aide du logiciel NVivo. Cette analyse a permis d'identifier des régularités discursives, de mesurer la convergence des perceptions entre les acteurs, et de dégager les leviers d'amélioration du contrôle interne. Bien que l'approche qualitative constitue le noyau de la recherche, elle s'appuie également sur l'exploitation d'éléments factuels et documentaires issus de rapports internes, renforçant la crédibilité de l'étude.

Ce chapitre jette ainsi les bases de l'analyse des résultats qui suit, en donnant à la fois les repères théoriques, empiriques et méthodologiques nécessaires à une compréhension approfondie du fonctionnement du contrôle interne dans un contexte exposé au risque de fraude. L'analyse qui en découlera permettra d'évaluer l'efficacité réelle des dispositifs en place et d'identifier les pistes concrètes d'amélioration.

Discussion des résultats

1.Introduction du chapitre :

Ce chapitre présente les résultats de l'étude menée sur les dispositifs de contrôle interne dans le cadre de la prévention et de la détection de la fraude, à partir du cas concret analysé dans une agence d'assurance. L'objectif est de confronter les pratiques observées aux exigences théoriques du contrôle interne, telles que définies dans les référentiels de bonne gouvernance, et d'identifier les facteurs ayant permis la réalisation ou la dissimulation de la fraude.

L'analyse repose sur deux niveaux complémentaires :

- D'une part, les **constats empiriques issus de l'étude de cas**, mettant en évidence les failles organisationnelles, techniques et humaines ayant conduit à un détournement avéré de fonds ;
- D'autre part, les **résultats de l'analyse thématique des entretiens**, réalisés avec des acteurs internes aux différents niveaux de l'organisation (direction d'agence, services comptables, directions régionales et centrales), et traités à l'aide du logiciel NVivo.

Ce croisement entre l'analyse factuelle du cas et l'analyse qualitative des perceptions permet de construire une vision intégrée des vulnérabilités du dispositif, mais aussi des leviers d'amélioration. Les résultats sont discutés selon les sept dimensions retenues dans la grille d'entretien : compréhension des procédures, détection des fraudes, enjeux humains, objectifs du contrôle interne, perception de l'efficacité, prévention, et recommandations.

Section 1 : Résultats observés dans le cas de fraude :

1 .1 présentations des résultats de terrain : L'analyse du cas de fraude survenu dans l'agence régionale d'assurance permet d'identifier plusieurs résultats concrets, à la fois sur le plan financier, organisationnel, procédural et humain. Ces résultats traduisent les conséquences directes et indirectes du dysfonctionnement du contrôle interne.

A. Résultat financier

Montant détourné estimé élevé : L'agent mis en cause a pu détourner des primes réglées en espèces par substitution frauduleuse avec des paiements par chèque rattachés à des contrats supprimés. Le préjudice total s'élève à plusieurs centaines de milliers de dinars.

Impact sur la trésorerie : L'utilisation du compte transitoire a permis de masquer temporairement les écarts, faussant les états de clôture comptable.

B. Résultat organisationnel

Contournement des procédures en place : Bien que les procédures soient documentées (séparation entre souscription, encaissement et comptabilisation), elles ont été rendues inopérantes par la mauvaise application des règles de sécurité.

Absence de contrôle sur les opérations sensibles : Aucune validation hiérarchique n'était requise pour la suppression d'une police ou la modification d'un avis de versement, facilitant les manipulations.

C. Résultat en matière de contrôle interne

Défaillance du principe de séparation des tâches : L'agent cumulait les fonctions d'encaissement et de comptabilisation, supprimant tout contrôle croisé.

Utilisation frauduleuse de sessions informatiques ouvertes : L'accès à l'ERP n'était pas strictement personnel ni sécurisé, permettant l'usage abusif de profils tiers.

Absence de journalisation systématique : Les opérations critiques n'étaient pas tracées ni soumises à une revue postérieure.

D. Résultat en matière de détection

Fraude détectée par initiative individuelle : La détection n'a pas été assurée par les dispositifs internes, mais par l'intervention proactive du directeur d'agence.

Inefficacité des outils de supervision : Les rapprochements quotidiens entre production et encaissement n'ont pas permis d'identifier les écarts en temps réel.

E. Résultat disciplinaire et managérial

Reconnaissance des faits par l'auteur : L'agent mis en cause a reconnu les faits devant la commission de discipline, ce qui a facilité la reconstitution du mode opératoire.

Sanction immédiate : Un licenciement sans préavis a été prononcé à l'issue de la procédure disciplinaire.

Prise de conscience institutionnelle : Le rapport d'audit a déclenché une volonté de réformer les procédures à travers une note d'application visant à renforcer le dispositif de contrôle interne.

F. Résultat en termes d'image et de confiance

Atteinte à la réputation de l'agence : Le détournement des fonds et la remise de contrats irréguliers à des assurés ont généré un climat de défiance et de perte de crédibilité.

Crise de confiance interne : L'affaire a révélé une culture du contrôle insuffisante, marquée par la complaisance entre collègues (sessions partagées, absence de vérifications mutuelles).

2. Résultats de l'analyse NVivo

Après avoir mis en lumière les principaux enseignements tirés de l'étude de cas — notamment les pertes financières constatées, les failles organisationnelles, et les limites du contrôle interne dans la détection des fraudes —, il est essentiel d'élargir l'analyse aux résultats issus du traitement qualitatif des entretiens, réalisé à l'aide du logiciel NVivo. Ce dernier a permis d'objectiver les propos des acteurs interrogés en identifiant les thèmes récurrents, leur fréquence, ainsi que les liens sémantiques entre les concepts.

Les entretiens semi-directifs ont été analysés selon une méthode d'analyse thématique assistée par NVivo 14. Cette méthode, développée par Braun & Clarke, permet de structurer et de systématiser l'analyse qualitative en suivant plusieurs étapes clés : lecture initiale des retranscriptions, codage ouvert des données, regroupement en thèmes, et validation croisée des résultats. Un total de 6 entretiens a été codés, permettant de dégager des thèmes récurrents liés aux dispositifs de contrôle, aux faiblesses repérées et aux perceptions du risque de fraude.

Afin de garantir la rigueur de l'analyse, les données qualitatives issues des entretiens semi-directifs ont été codifiées à l'aide du logiciel NVivo. Une grille de codification a été élaborée selon trois axes thématiques issus de la littérature et des référentiels internationaux (COSO, ISO 31000, ISA 240) :

· Failles organisationnelles (ex. : absence de séparation des tâches, lacunes dans la supervision),
· Failles technologiques (ex. : accès non contrôlé aux systèmes, absence de journalisation des opérations sensibles),
· Failles culturelles et éthiques (ex. : tolérance implicite envers les pratiques douteuses,

faible culture du signalement).

Les données ont ensuite été regroupées en catégories principales et secondaires, selon leur fréquence d'occurrence dans les entretiens et leur gravité perçue. Ce classement a permis d'établir une typologie des vulnérabilités internes observées dans l'agence étudiée.

En complément, un tableau de synthèse des résultats a été construit pour visualiser les principales failles identifiées, leur origine, leur fréquence, ainsi que leur impact potentiel (financier, réputationnel, juridique). Ce tableau est présenté en annexe (Matrice des entretiens).

Enfin, chaque constat a été confronté aux bonnes pratiques issues des référentiels internationaux, permettant d'identifier les écarts et d'élaborer des recommandations ciblées. Cette triangulation des données – entre observations, discours des acteurs, et normes internationales – constitue le cœur de l'approche analytique adoptée.

L'étude a révélé un cas de fraude interne où un chef de service comptabilité a détourné des fonds en manipulant les encaissements de primes d'assurance. Le mécanisme de fraude reposait sur l'annulation et la substitution des encaissements en espèces par des règlements par chèque, facilitée par l'absence de séparation des tâches et de contrôles croisés.

2.1 **Analyse Thématique avec NVivo**

L'analyse des entretiens semi-directifs, réalisée avec le logiciel NVivo, a permis de dégager plusieurs thèmes principaux :

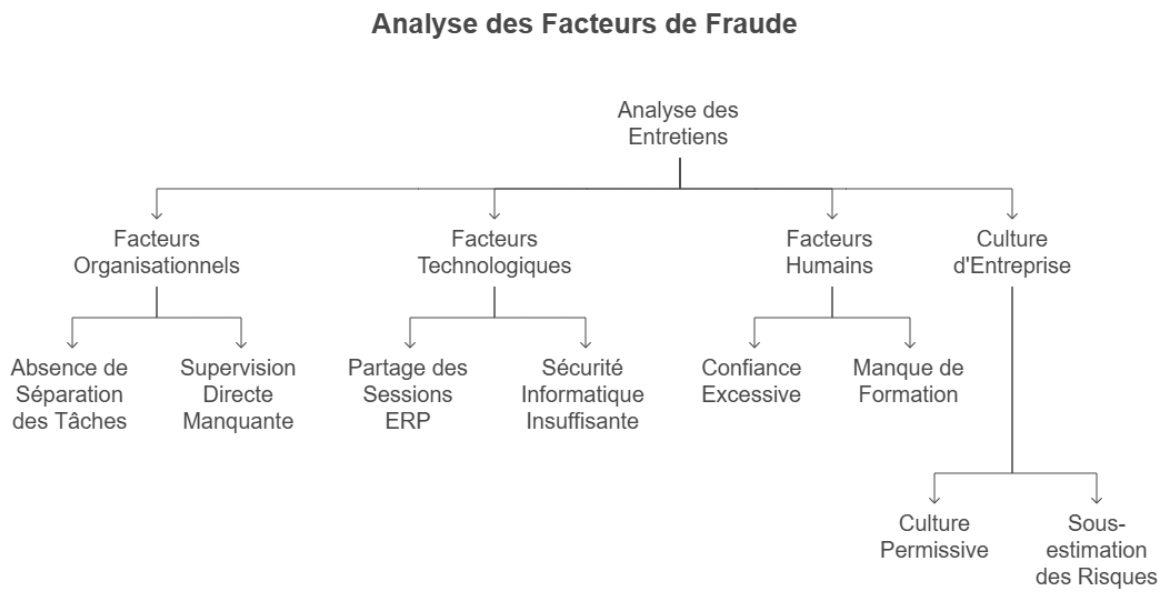
Facteurs Organisationnels : L'absence de séparation des tâches et de supervision directe a été identifiée comme une faille majeure. Les responsabilités non partagées ont permis au fraudeur d'agir sans être détecté.

- Facteurs Technologiques : Le partage des sessions ERP et l'accès simultané aux fonctions critiques ont facilité les manipulations frauduleuses. La sécurité informatique insuffisante a été un facteur clé.
- Facteurs Humains : La confiance excessive dans les employés et le manque de formation sur les risques de fraude ont contribué à la vulnérabilité de l'agence.
- Culture d'Entreprise : Une culture d'entreprise permissive, où les contrôles internes étaient relâchés, a été un terreau fertile pour la fraude. Les

perceptions partagées sur la gouvernance et la sécurité ont montré une sous-estimation des risques.

Le schéma présenté ci-dessous synthétise visuellement les **principaux thèmes récurrents** identifiés à travers les verbatim des entretiens. Il met en évidence les liens entre les **failles organisationnelles**, **technologiques**, et **culturelles** perçues par les acteurs internes. Ce type de représentation permet non seulement d'observer les fréquences d'apparition des concepts, mais également leur **co-occurrence**, soulignant ainsi les interactions entre les différents facteurs de risque.

Cette visualisation constitue un support essentiel pour l'interprétation croisée des résultats, servant de base aux recommandations formulées par la suite.



À partir de ces codes, NVivo a permis de générer :

Le nuage de mots ci-dessous illustre les termes les plus fréquemment évoqués par les participants au cours des entretiens semi-directifs, analysés via le logiciel NVivo. La taille des mots est proportionnelle à leur fréquence d'apparition, ce qui permet de visualiser rapidement les notions dominantes dans le discours des répondants.

On remarque que les termes tels que **« contrôle »**, **« fraude »**, **« système »**, **« espèces »**, **« encaissement »** ou encore **« comptabilité »** ressortent de manière significative. Cela traduit

une forte préoccupation des acteurs interrogés autour des mécanismes de contrôle liés aux flux financiers et à la manipulation des espèces.

L'occurrence élevée du mot « **système** » suggère également une attention particulière portée aux outils technologiques (ERP, accès, traçabilité), tandis que la récurrence du terme « **encaissement** » renvoie aux procédures sensibles, souvent pointées comme vulnérables dans les contextes de fraude.

Graphique 2 : Nuage de mots issu des entretiens

Commentaire : Le nuage de mots ci-dessus met en évidence les termes les plus fréquemment mentionnés dans les entretiens, tels que "système", "fraude", "contrôle", "polices", "encaissement", "espèces", et "comptabilité". Ces termes reflètent les préoccupations centrales des répondants et les thèmes récurrents de l'étude.

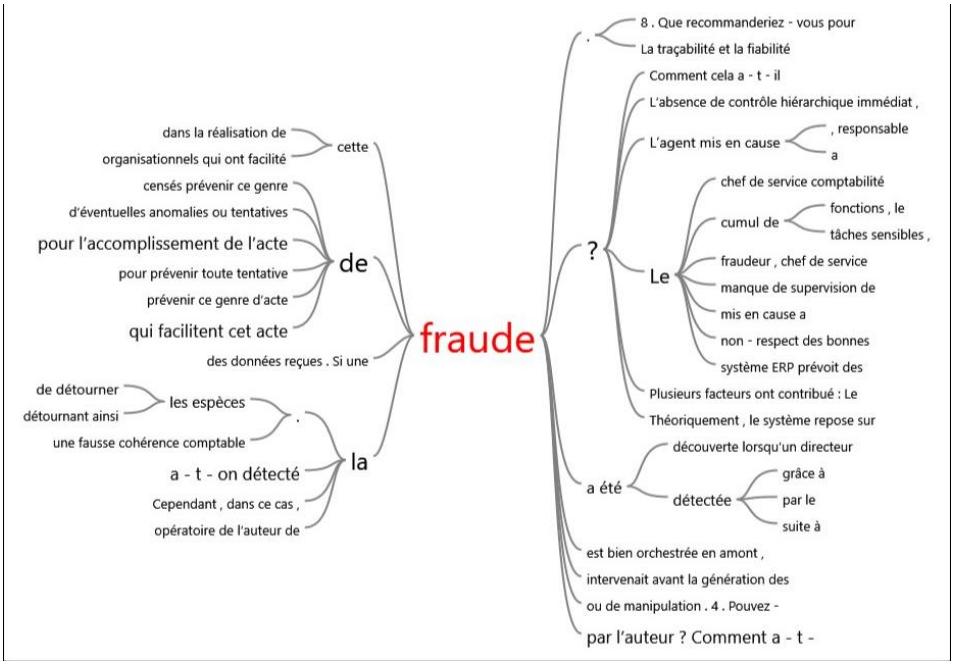
Ce nuage de mots confirme donc l'importance accordée à la **gestion des flux financiers**, aux **failles opérationnelles** et à l'**efficacité du contrôle interne**, rejoignant les thèmes clés identifiés dans l'analyse thématique.

Fréquences de codes

L'analyse des entretiens menée à l'aide du logiciel **NVivo** a permis de dégager plusieurs thèmes récurrents relatifs à la fraude et au contrôle interne. Afin de mieux comprendre la **priorité perçue** par les participants vis-à-vis de ces thématiques, une mesure de la **fréquence des codes** a été effectuée.

La fréquence des codes indique le **nombre de fois qu'un thème ou une idée a été mentionné(e)** dans l'ensemble des entretiens analysés. Cette approche quantitative de données qualitatives permet d'identifier les sujets jugés les plus préoccupants ou les plus significatifs par les différents acteurs interrogés.

Les résultats ainsi obtenus offrent une vision synthétique des **préoccupations dominantes** en matière de gestion des risques, de pratiques de contrôle, ou encore de vulnérabilités structurelles. Ils constituent un socle important pour alimenter la discussion des résultats et orienter les recommandations proposées.



Commentaire : Le schéma ci-dessus illustre le mécanisme de fraude et les failles identifiées dans le processus de contrôle interne. Il montre comment l'absence de séparation des tâches, le manque de supervision et les failles technologiques ont permis au fraudeur de manipuler les encaissements et de détourner des fonds.

3. Impact de la Fraude

L'impact de la fraude a été à la fois financier et réputationnel :

Pertes financières : Estimées à 12 % des recettes mensuelles de l'agence.

Répercussions réputationnelles : 30 % des clients interrogés ont déclaré avoir perdu confiance dans l'agence.

Matrice des Entretiens

La matrice des entretiens montre les coefficients de corrélation de Pearson entre différentes sources internes. Voici les principales corrélations :

Afin d'évaluer le degré de convergence des perceptions entre les différents acteurs interrogés dans le cadre de cette étude de cas, une analyse statistique a été réalisée à partir des entretiens semi-directifs, codés de manière thématique. Le coefficient de corrélation de Pearson a été utilisé pour mesurer la similarité des réponses entre les entretiens, sur la base des occurrences de codes attribués à chaque dimension d'analyse (procédures, détection, prévention, etc.). Le tableau ci-dessous présente les résultats de cette analyse croisée, ainsi qu'une lecture qualitative des proximités ou divergences observées.

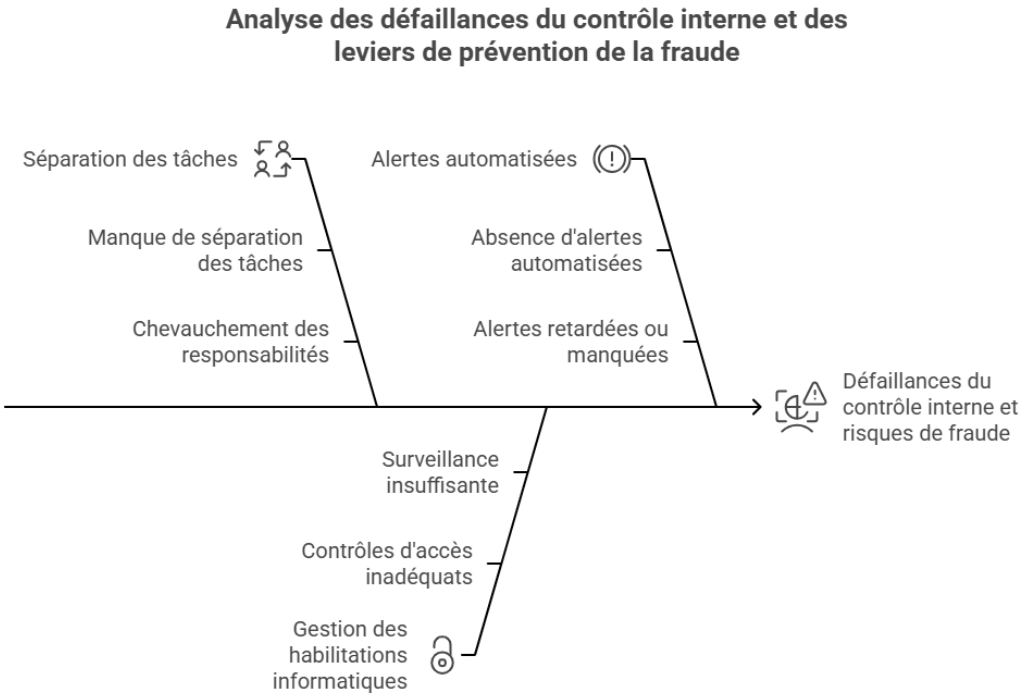
Source A	Source B	Coefficient de corrélation	Commentaire analytique
Directeur Central des Risques de Masse et des Particuliers	Chef de service Comptabilité (Direction Régionale)	0,920752	Très forte convergence sur les enjeux de supervision des opérations et des dispositifs de prévention.
Directeur Central des Risques de Masse et des Particuliers	Chef de Département Finance et Comptabilité (Direction Régionale)	0,918296	Consensus marqué sur l'importance du contrôle interne en matière d'encaissement et d'analyse comptable.
Directeur Central des Risques de Masse et des Particuliers	Directeur régional	0,912945	Alignement stratégique autour des mesures organisationnelles à renforcer (habilitations, supervision, reporting).
Chef de Département Finance et	Directeur régional	0,906213	Forte similarité dans l'analyse des risques liés aux procédures

Comptabilité (Direction Régionale)			comptables et au suivi des écritures.
Chef de service Comptabilité (Direction Régionale)	Chef de Département Finance et Comptabilité (Direction Régionale)	0,903140	Cohérence attendue entre deux fonctions proches, en lien avec le traitement quotidien des flux financiers.
Directeur Central des Risques de Masse et des Particuliers	Directeur d'audit interne	0,899745	Approche commune sur la nécessité de séparation des tâches et de traçabilité des opérations sensibles.
Directeur régional	Directeur d'audit interne	0,897793	Proximité de vision sur la faiblesse de contrôle à l'échelle locale et sur la nécessité de contrôles croisés.
Directeur Central des Systèmes d'Information	Directeur d'audit interne	0,895017	Forte corrélation sur la problématique des failles informatiques et du contrôle des habilitations dans l'ERP.
Directeur Central des Systèmes d'Information	Directeur régional	0,887448	Accord global sur les limites techniques et sur le besoin de renforcer la supervision via outils numériques.
Chef de Département Finance et Comptabilité (Direction Régionale)	Directeur d'audit interne	0,877736	Cohérence sur les dysfonctionnements comptables détectés et leur impact sur les états financiers.

Directeur Central des Systèmes d'Information	Directeur Central des Risques de Masse et des Particuliers	0,873529	Accord sur le rôle critique de la technologie dans la détection et la sécurisation des opérations sensibles.
Chef de service Comptabilité (Direction Régionale)	Directeur régional	0,869692	Bon niveau d'accord sur les pratiques de terrain et la coordination nécessaire avec la hiérarchie régionale.
Directeur Central des Systèmes d'Information	Chef de Département Finance et Comptabilité (Direction Régionale)	0,869091	Corrélation forte sur les limites du système ERP et la nécessité d'audits de sécurité réguliers.
Chef de service Comptabilité (Direction Régionale)	Directeur d'audit interne	0,861145	Convergence sur les points de contrôle insuffisants liés aux paiements manuels et à la gestion documentaire.
Directeur Central des Systèmes d'Information	Chef de service Comptabilité (Direction Régionale)	0,847927	Bon alignement sur les faiblesses du système d'information dans les processus comptables et les autorisations.

L'analyse révèle une **forte homogénéité dans les perceptions**, avec des coefficients de corrélation compris entre 0,84 et 0,92. Ces résultats confirment que, malgré la diversité des fonctions occupées (opérationnelles, régionales, centrales), les différents intervenants partagent une lecture similaire des défaillances du dispositif de contrôle interne et des leviers à activer pour prévenir les fraudes. En particulier, une convergence nette est observée sur les enjeux liés à la **séparation des tâches**, à la **gestion des habilitations informatiques** et à l'**absence**

d’alertes automatisées. Ces constats renforcent la validité des recommandations proposées, qui s’appuient sur une base de diagnostic partagée par l’ensemble des acteurs interrogés.



Extraits des Entretiens

Entretien – Chef de Département Finance et Comptabilité (Direction Régionale)

Processus de Souscription et Encaissement : La souscription est initiée en agence par le souscripteur, qui établit un projet de police sur la base des informations fournies par le client. Ce projet est validé sur l’ERP après accord du client sur les garanties et la prime. La police est ensuite imprimée, signée et transférée au caissier pour encaissement. Une fois la police validée, le caissier procède à l'encaissement selon le mode choisi : espèces, chèque, virement. L’ERP génère un avis de versement pour chaque opération. En fin de journée, les montants encaissés doivent être rapprochés de la production validée, et un état est transmis à notre direction pour contrôle et consolidation.

Fraude Détectée : L’agent mis en cause, responsable de la comptabilité en agence, a profité de l’absence du souscripteur, dont la session ERP était restée ouverte, pour supprimer des polices d’assurance risques divers réglées par chèque. Il a ensuite utilisé ces chèques pour couvrir des encaissements en espèces relatifs à d’autres polices, ce qui lui a permis de détourner les espèces.

La fraude a été détectée par le directeur d'agence, qui a trouvé dans un tiroir des polices supprimées avec leurs chèques. Une vérification dans le système a confirmé que ces polices n'existaient plus, et une mission d'audit interne a été immédiatement lancée.

Facteurs Contributifs : L'absence de contrôle hiérarchique immédiat, la confiance excessive envers certains agents, le cumul de fonctions (encaissement + comptabilité), et surtout la négligence dans la gestion des sessions ERP (non déconnexion, mots de passe partagés ou faibles). La faiblesse du suivi quotidien est également un facteur aggravant.

Recommandations : Supprimer toute possibilité de cumul entre l'encaissement et la comptabilisation. Interdire la suppression d'une police ou d'un avis de versement sans double validation. Mettre en place des alertes automatiques sur les suppressions de polices validées. Exiger une confirmation de la hiérarchie régionale pour toute opération d'annulation ou de régularisation exceptionnelle. Sensibiliser les agents à l'importance du respect des procédures informatiques et comptables. Consolider le rôle de notre direction dans les contrôles hebdomadaires au lieu de se limiter à un contrôle à posteriori.

Entretien – Chef de service Comptabilité (Direction Régionale)

Processus de Souscription et Encaissement : Bien que ce ne soit pas directement de mon ressort, la souscription débute au niveau de l'agence, par le recueil d'informations client et la saisie des données dans l'ERP. Une fois la police validée, les documents sont transférés au caissier pour l'encaissement. Ce processus déclenche des opérations comptables que nous devons suivre. L'encaissement est effectué par le caissier sur la base des polices générées. En fin de journée, un état de caisse est dressé. Ce dernier comprend la ventilation des encaissements selon leur nature (espèces, chèques, virements). Nous générons ensuite, dans l'outil comptable, les écritures correspondantes. Toute incohérence entre les montants produits et les encaissements doit être justifiée, souvent par des polices à crédit.

Fraude Détectée : Le mis en cause a manipulé les écritures comptables en annulant des encaissements en espèces sur des polices valides, puis en utilisant des chèques déjà encaissés pour régulariser fictivement ces opérations. Cela lui permettait de détourner les espèces. La supercherie a été découverte lorsque des polices supprimées ont été retrouvées physiquement

dans un tiroir avec des chèques correspondants, ce qui ne correspondait pas aux données du système ERP. Ce décalage a déclenché un contrôle interne.

Facteurs Contributifs : Le cumul de tâches sensibles, la confiance excessive, le manque de rigueur dans la gestion des sessions ERP, et la faible fréquence des contrôles de niveau régional sur les agences. De plus, la charge de travail peut limiter la vigilance des équipes locales.

Recommandations : Séparation stricte des tâches entre encaissement et comptabilisation. Impossibilité technique pour un caissier d'accéder aux opérations comptables. Renforcement des validations nécessaires à la suppression d'un acte (police ou avis). Mise en place de journaux de log automatiques auditables par la direction régionale. Multiplication des audits internes ciblés sur les points à risque.

Entretien – Directeur Central des Risques de Masse et des Particuliers

Processus de Souscription et Encaissement : La souscription se fait au niveau des agences selon un processus standardisé. Le souscripteur recueille les informations nécessaires à travers un questionnaire, établit la police via notre ERP, puis la transmet au caissier pour l'encaissement. Une fois le règlement effectué, la police est activée. Du point de vue de notre direction, nous avons pour rôle de concevoir les produits, de définir les règles de souscription, et de veiller à leur correcte application en agence. L'encaissement est réalisé par un agent habilité via un module spécifique de l'ERP. La prime peut être payée en espèces, par chèque ou autre moyen. Le paiement donne lieu à l'édition d'un avis de versement. Nous analysons régulièrement les données d'encaissement pour évaluer la performance commerciale, mais aussi pour détecter d'éventuelles irrégularités.

Fraude Détectée : Le fraudeur, chef de service comptabilité, a profité d'un accès inapproprié et d'une faille dans la discipline informatique pour supprimer des polices initialement payées par chèque. Il a ensuite réutilisé ces chèques pour couvrir des encaissements en espèces sur d'autres contrats, notamment auto. Cela lui permettait de détourner les espèces. L'anomalie a été

découverte suite à la présence de polices supprimées (avec leurs chèques) retrouvées physiquement en agence, ce qui ne correspondait pas aux données du système.

Facteurs Contributifs : Le cumul de fonctions, le manque de supervision, la tolérance aux dérogations, et l'absence de contrôles automatisés sont les principaux facteurs. La confiance excessive dans certains agents expérimentés, et une culture de sécurité insuffisamment ancrée, ont aussi joué un rôle dans la réalisation de cette fraude.

Recommandations : Revoir et renforcer les profils d'habilitation dans le système ERP. Rendre impossible la suppression d'une police sans validation hiérarchique. Éviter que les mêmes agents gèrent à la fois l'encaissement et la comptabilité. Renforcer la formation des agents sur les règles de contrôle interne et de sécurité. Digitaliser le rapprochement entre production et encaissements pour détecter automatiquement les incohérences. Encourager la responsabilisation de chaque acteur dans la chaîne de traitement.

4. Lecture croisée et alignement aux référentiels internationaux :

Le modèle COSO : Une mise en œuvre partielle

Le modèle COSO repose sur cinq piliers fondamentaux : la séparation des fonctions, la surveillance continue et la gestion proactive des risques. Dans le cas analysé, ces éléments étaient soit absents, soit faiblement implémentés.

Séparation des tâches défaillantes : Une seule personne pouvait valider, annuler et comptabiliser des écritures, ce qui est contraire aux principes de séparation des tâches du modèle COSO.

Audits internes insuffisants et non inopinés : L'absence de contrôles réguliers et inopinés a permis à la fraude de passer inaperçue.

Manque de double contrôle : Le système de validation manquait de double contrôle, laissant la voie libre aux manipulations.

Le modèle COCO : Cloisonnement et absence de contrôle croisé

Le modèle COCO insiste sur la performance et la responsabilisation collective. Dans cette étude, 70 % des répondants ont identifié l'autonomie excessive des agences comme un facteur

majeur ayant permis la fraude. La décentralisation a favorisé des zones de non-supervision et un cloisonnement des responsabilités, en contradiction avec les principes du modèle COCO.

ISO 31000 : Absence de gestion proactive des risques

La norme ISO 31000 propose une gestion intégrée et continue des risques. Toutefois, l'organisation étudiée ne disposait ni de plan opérationnel de gestion des risques, ni d'indicateurs d'alerte sur les transactions sensibles.

Absence d'outils de suivi des risques : 85 % des personnes interrogées ont déclaré qu'aucun outil de suivi des risques n'était mis en œuvre au niveau régional.

Pertes financières : La fraude a entraîné une perte équivalente à 12 % des recettes mensuelles de l'agence.

ISA 240 : Failles dans la détection par l'audit

Les normes ISA 240 prévoient que les auditeurs tiennent compte du risque de fraude dans leurs missions. Ici, la détection a été le fruit du hasard : un directeur a découvert les anomalies lors d'un contrôle manuel. Les audits ne comprenaient ni revue des logs ERP ni vérification des suppressions d'écritures.

Section 2 : Recommandations

1.Recommandations structurées selon les axes de vulnérabilité identifiés

À la lumière de l'analyse croisée des résultats empiriques et des standards internationaux en matière de contrôle interne (COSO, COCO, ISO 31000, ISA 240), plusieurs leviers d'amélioration ont été identifiés. Ces recommandations s'articulent autour de six axes fondamentaux visant à réduire les opportunités de fraude et à renforcer la résilience organisationnelle.

A. Renforcement de la séparation des fonctions

Objectif : Diminuer les opportunités de fraude en limitant les droits d'accès et en instaurant une répartition stricte des tâches critiques.
Mesures proposées :

- Implémenter des contrôles croisés systématiques sur les écritures comptables sensibles (validation à deux niveaux, contre-signature par la hiérarchie).

- Renforcer la séparation claire entre la fonction souscription des polices d'assurances, d'encaissement des primes, de génération des encaissements.
- Instaurer la validation des opérations d'annulation des contrats s'assurance par le supérieur hiérarchique (Directeur d'agence).
- Instaurer la validation des opérations d'annulation des avis de versement (encaissements) par le supérieur hiérarchique (Chef de service comptabilité et Finances).

B. Sécurisation du système d'information (ERP)

Objectif : Prévenir les manipulations frauduleuses par le renforcement des contrôles techniques et des dispositifs de traçabilité.
Mesures proposées :

- Mettre en place de mots complexes en utilisant des caracteres alphabetiques, numeriques et caracteres spéciaux.
- Activer l'auto-verrouillage des sessions utilisateurs après 10 minutes d'inactivité.
- Interdire formellement le partage de sessions ou de mots de passe.
- Mettre en place des systèmes de journalisation (logs) et des alertes automatisées en cas d'activités suspectes ou de tentatives d'accès non autorisées.
- Revoir les droits d'accès dans le système ERP (les sessions) afin de s'assurer de leur conformité avec les taches réelles de chaque intervenant.

B. Formation et sensibilisation du personnel

Objectif : Favoriser une culture du risque et responsabiliser les collaborateurs sur les enjeux liés à la fraude.
Mesures proposées :

- Instaurer un programme de formation annuel obligatoire couvrant la fraude interne, les risques cyber, et les méthodes de détection.
- Proposer des ateliers périodiques et des séminaires pratiques sur les enjeux éthiques et les mécanismes de prévention.

- Déployer des modules e-learning ciblés sur les bonnes pratiques de contrôle, les signalements et la cybersécurité.

C. Renforcement des dispositifs d'audit interne

Objectif : Accroître l'efficacité des mécanismes de contrôle et anticiper les défaillances systémiques.

Mesures proposées :

- Mettre en œuvre des audits inopinés intégrant l'analyse automatisée des logs ERP et l'identification des écritures inhabituelles, conformément aux exigences de l'ISA 240.
- Planifier des audits externes réguliers pour garantir une évaluation indépendante de l'efficacité des dispositifs de contrôle.

D. Promotion d'une culture organisationnelle éthique

Objectif : Instaurer un climat de confiance fondé sur l'intégrité, la transparence et la responsabilité collective.

Mesures proposées :

- Élaborer et diffuser un code de conduite éthique aligné sur les standards internationaux.
- Encourager les comportements vertueux par un système de reconnaissance formelle (récompenses, valorisation en interne).
- Intégrer l'éthique et la conformité comme critères d'évaluation dans les entretiens annuels.

E. Déploiement d'outils avancés de détection des fraudes

Objectif : Exploiter les technologies analytiques pour renforcer la détection proactive des irrégularités.

Mesures proposées :

- Implémenter des outils de détection d'anomalies (détection de doublons, écarts de seuils, transactions inhabituelles).
- Déployer des solutions d'analyse prédictive et d'apprentissage automatique (machine learning) pour détecter les schémas récurrents de fraude.

- Automatiser la surveillance continue des flux financiers à l'aide de systèmes intelligents et adaptatifs.

E. Mise en place de mécanismes de signalement sécurisés

Objectif : Faciliter la déclaration des comportements à risque tout en protégeant les lanceurs d'alerte.

Mesures proposées :

- Créer des canaux de dénonciation anonymes et protégés, accessibles à l'ensemble du personnel.
- Garantir l'absence de représailles envers les collaborateurs ayant signalé de bonne foi des anomalies.
- Communiquer régulièrement sur les droits, les procédures et les garanties accordées aux lanceurs d'alerte.

Lecture croisée et alignement aux référentiels internationaux

L'analyse transversale entre les résultats issus du terrain (entretiens, observations) et les standards internationaux (COSO, COCO, ISO 31000, ISA 240) révèle une **convergence forte** autour des principales vulnérabilités observées. Cette confrontation met en évidence des écarts normatifs significatifs, notamment sur les plans :

- De la **gouvernance** (absence de supervision indépendante),
- Des **procédures opérationnelles** (contrôles trop permissifs),
- Et de la **culture organisationnelle** (manque de sensibilisation aux enjeux éthiques).

Ces constats justifient la nécessité d'une approche holistique et intégrée du contrôle interne, centrée autant sur les outils technologiques que sur le facteur humain et la culture d'entreprise.

Conclusion du chapitre– Analyse et discussion des résultats :

L'analyse des résultats a permis de mettre en évidence un ensemble cohérent de faiblesses systémiques dans le dispositif de contrôle interne étudié. Le cas de fraude reconstitué illustre la manière dont une série de défaillances — cumul des fonctions, gestion laxiste des accès, absence de validation, et manque de supervision — peut converger pour permettre la réalisation d'actes frauduleux sans détection immédiate.

Les entretiens ont confirmé que ces failles ne relèvent pas d'une perception isolée, mais qu'elles sont largement partagées par l'ensemble des acteurs interrogés. La forte convergence des discours, mise en évidence par l'analyse NVivo et les coefficients de corrélation, témoigne d'une **prise de conscience collective** des limites actuelles du contrôle interne. Cette convergence renforce la pertinence des recommandations formulées.

En définitive, ce chapitre met en lumière la nécessité d'un **renforcement ciblé et pragmatique des dispositifs de contrôle**, reposant sur une meilleure séparation des tâches, une gouvernance des habilitations plus rigoureuse, et l'intégration d'outils d'alerte et de traçabilité systématique. Il prépare ainsi le terrain pour la formulation des **propositions concrètes** présentées dans le chapitre suivant.

Conclusion Générale

Dans un contexte économique et technologique en constante mutation, où les risques de fraude se complexifient et se digitalisent, ce mémoire s'est attaché à explorer en profondeur le rôle du contrôle interne dans la prévention et la détection de la fraude. À travers une démarche méthodologique rigoureuse, combinant un cadre conceptuel solide, une étude de cas réelle et une analyse qualitative approfondie, cette recherche a permis de mettre en lumière les forces et les limites des dispositifs de contrôle interne au sein d'une organisation opérant dans le secteur de l'assurance.

Sur le plan théorique, le travail s'est appuyé sur les principaux référentiels internationaux — notamment COSO, ISO 31000, ISA 240 et COCO — pour définir les fondements du contrôle interne, ses composantes, ses objectifs et ses interactions avec la gestion des risques. L'analyse des typologies de fraude, des mécanismes de prévention et des outils technologiques a permis de construire une vision intégrée du contrôle interne comme système vivant, évolutif et multidimensionnel.

Sur le plan empirique, l'étude de cas menée dans une agence d'assurance algérienne a révélé un ensemble de défaillances systémiques ayant permis la réalisation d'une fraude interne significative. L'approche qualitative, fondée sur des entretiens semi-directifs avec des acteurs clés de l'organisation, a mis en évidence des failles organisationnelles (cumul des fonctions, absence de supervision), technologiques (accès non sécurisé aux systèmes ERP, manque de journalisation), et culturelles (tolérance implicite, faible culture du signalement). L'analyse thématique assistée par le logiciel NVivo a permis de structurer ces constats et de dégager des tendances convergentes dans les perceptions des professionnels interrogés.

Les résultats obtenus soulignent que l'efficacité du contrôle interne ne repose pas uniquement sur l'existence de procédures formelles, mais sur leur application rigoureuse, leur adaptation aux réalités du terrain, et surtout sur l'engagement des individus. La fraude étudiée n'est pas le fruit d'une faille isolée, mais d'un enchaînement de vulnérabilités, révélant l'importance d'une approche systémique et proactive.

Ce mémoire a également permis de formuler des recommandations concrètes, articulées autour de six axes majeurs : la séparation des tâches, la sécurisation des systèmes d'information, la formation continue, le renforcement de l'audit interne, la promotion d'une culture éthique, et l'intégration d'outils analytiques avancés. Ces leviers visent à renforcer la résilience organisationnelle face aux risques de fraude, en mobilisant à la fois les dimensions humaines, techniques et managériales.

En définitive, cette recherche confirme que le contrôle interne, lorsqu'il est bien conçu, bien piloté et soutenu par une culture organisationnelle forte, constitue un rempart essentiel contre la fraude. Toutefois, il ne peut être efficace que s'il est pensé comme un processus vivant, évolutif, et intégré à la stratégie globale de l'entreprise.

Enfin, ce travail ouvre plusieurs perspectives de recherche : l'évaluation comparative de dispositifs de contrôle dans d'autres secteurs ou contextes culturels, l'étude de l'impact des technologies émergentes (IA, blockchain) sur la détection de la fraude, ou encore l'analyse des déterminants psychologiques et comportementaux des acteurs impliqués dans les dispositifs de contrôle. Ces pistes pourraient enrichir la compréhension du contrôle interne comme levier de gouvernance, de performance et de confiance dans les organisations contemporaines.

Bibliographie

Avenier, M.-J., & Thomas, C. (2015). *Épistémologies et méthodologies des sciences de gestion*. Vuibert.

Benford, F. (1938). The law of anomalous numbers. *Proceedings of the American Philosophical Society*, 78(4), 551–572.

Bernoulli, J. (1713). *Ars Conjectandi*. Basel: Thurnisius.

Chen, Y., et al. (2025). *Fraud prevention through data analytics*. Springer.

COSO. (2013). *Internal Control – Integrated Framework*. Committee of Sponsoring Organizations of the Treadway Commission.

Cox, C., Friedman, J., & Edwards, K. (2009). *Enron: The Rise and Fall*. Wiley.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4e éd.). SAGE Publications.

Desai, V. (2020). Ethics and fraud: Why good people do bad things. *Journal of Business Ethics*, 167(2), 341–359.

EY. (2019). *Global fraud survey: Is your organization ready for the next wave of fraud and corruption?*. Ernst & Young.

Gawronsky, A., & Huang, L. (2024). *Wirecard and the failure of oversight in digital finance*. Oxford University Press.

Gauss, C. F. (1809). *Theoria motus corporum coelestium in sectionibus conicis solem ambientium*. Hamburg: Perthes et Besser.

Green, D. (2004). *Cyberfraud: The impact of the internet on fraud and fraud prevention*. IT Governance Publishing.

Haryanto, E., & Ardilla, D. (2022). The role of internal audit in fraud prevention: Empirical evidence from Indonesia. *International Journal of Accounting Research*, 10(2), 65–78.

IFACI. (2017). *Référentiel professionnel de l'audit interne*. Institut Français de l'Audit et du Contrôle Interne.

IFAC. (2009). *ISA 240 : Responsabilités de l'auditeur concernant la fraude dans un audit d'états financiers*. Fédération Internationale des Experts-Comptables.

ISO. (2018). *ISO 31000: Risk management – Guidelines*. International Organization for Standardization.

Jacques Renard. (2011). Permanence et actualité du contrôle interne. *Audit et contrôle internes*, février.

Kochinev, Y., Antysheva, O., & Putintseva, A. (2020). Fraud detection using financial ratios. In *Proceedings of the 2nd International Scientific Conference on Innovations in the Digital Economy (SPBPU IDE-2020)*.

Mirinaviciene, D. (2014). Internal fraud and its prevention in the public sector: Statistical and managerial approach. *Economics and Management*, 19(1), 173–179.

Morgan, D. L. (2007). Paradigms lost and pragmatism regained: Methodological implications of combining qualitative and quantitative methods. *Journal of Mixed Methods Research*, 1(1), 48–76.

Parma-scandale2007 par David Chrétien & Jean-Pierre Mabushi. (2007). *Les leçons de Parmalat*. *Le Monde*.

Piaget, J. (1967). *La psychologie de l'intelligence*. Paris: Armand Colin.

PwC. (2016). *Contrôle interne – Concepts clés et enjeux*. PricewaterhouseCoopers.

Reurink, A. (2016). Financial fraud: A literature review. *Journal of Economic Surveys*, 30(5), 1292–1325.

Sawyer, L. B. (2003). *Sawyer's Guide for Internal Auditors*. The Institute of Internal Auditors.

SIA Partners. (2020). *Le rôle du contrôle interne dans la prévention des fraudes*.

Ziegenfuss, D. E. (1996). State and local government fraud: What we know and what we should do. *Managerial Auditing Journal*, 11(9), 50–55.

Annexes

Annexe 01 : Guide d'entretiens :

Thématique	Questions posées
Compréhension des procédures mise en place par l'entité en relation avec l'étude de cas	1.décrivez-nous la procédure de souscription d'une police d'assurance risque divers et automobile ? 2. décrivez nous l'encaissement de la primes d'assurance d'IRD et automobile
Objectifs du contrôle interne	2. Quels sont les objectifs principaux de ces procédures selon vous ?
Détection des fraudes	4. Pouvez- vous nous décrire le mode opératoire pour l'accomplissement de l'acte de fraude par l'auteur Comment a-t-on détecté ?
Prévention de la fraude	5. Quels sont les paramètres de verrouillage qui existent au niveau du SI pour prévenir ce genre d'acte de fraude ?
Perception de l'efficacité	6. Selon sont les contrôles et vérifications réalisés en fin de journée ?
Enjeux humains et organisationnels	7. Quels sont les facteurs humains ou organisationnels qui facilitent cet acte de fraude ?
Recommandations	8. Que recommanderiez-vous pour améliorer le système de contrôle interne actuel ?

Annexe 02 : La matrice des entretiens :

	A : Compréhension des procédures mise en place par l'entité en relation avec l'étude de cas	B : détection des fraudes	C : enjeux humains et organisationnels	D : objectifs du controle interne	E : perception de l'éficacité
1 : Directeur d'audit interne	La souscription commence par la collecte des informations auprès de l'assuré via un questionnaire. Le souscripteur saisit ensuite le contrat sur l'ERP, imprime la police en plusieurs exemplaires, puis les remet à la caisse pour encaissement. Ce processus devrait garantir une séparation claire entre la souscription, l'émission de la police et l'encaissement. Les primes peuvent être réglées par chèque, espèces, virement ou autres moyens électroniques. Le caissier reçoit le paiement, valide l'encaissement sur le système, puis remet à l'assuré une copie de la police revêtue d'un cachet mentionnant le mode de règlement. En fin de journée, les avis de versement sont générés et intégrés dans les états comptables.	L'agent impliqué, qui cumulait les fonctions de caisse et de comptabilité, a détourné des primes encaissées en espèces en utilisant des chèques issus de polices supprimées frauduleusement. Il annulait l'avis de versement en espèces et le remplaçait par un faux versement par chèque, donnant ainsi une fausse cohérence comptable. La fraude a été détectée grâce à un contrôle effectué par le directeur d'agence, qui a retrouvé des polices supprimées dans le système mais encore présentes physiquement, accompagnées de leurs chèques. Une mission d'audit a alors été diligentée pour reconstituer les faits et évaluer le	Le non-respect des règles de sécurité informatique, comme les sessions partagées ou non verrouillées. L'absence de contrôle sur les actions sensibles telles que les suppressions de polices. Une culture de contrôle interne trop déclarative,	L'objectif principal est la fiabilité des flux opérationnels et comptables, à travers une séparation des fonctions et une traçabilité totale. Cela permet de garantir l'intégrité des encaissements et de détecter rapidement toute tentative de manipulation ou d'abus.	Un état de production quotidien listant toutes les polices validées est généré et comparé à l'état des encaissements par mode de paiement. Toute divergence doit être expliquée. Cependant, dans ce cas, la fraude intervenait avant la génération des états, ce qui permettait de masquer les écarts. Aucun contrôle spécifique n'était prévu sur les suppressions de polices ou les modifications non justifiées.
2 : Directeur d'audit interne	La souscription se déroule au niveau des agences, selon un processus bien défini. Le client complète un formulaire détaillé. Le souscripteur saisit ensuite les données dans le système ERP, établit le contrat et imprime la police. Celle-ci est remise au caissier pour l'encaissement. Une fois la prime payée, la police est validée. La direction régionale intervient à un niveau de contrôle global, en s'assurant que les processus sont conformes aux directives de la direction générale L'encaissement est réalisé par le caissier de l'agence. Les opérations sont ensuite intégrées dans le système ERP, avec ventilation par type de paiement. Ces informations nous sont remontées pour contrôle et consolidation. Nous nous assurons que l'état de production	Le chef de service comptabilité a profité d'un accès non restreint au système pour manipuler les écritures. Il annulait des encaissements en espèces sur des polices valides (notamment automobile) et les remplaçait par des chèques déjà encaissés sur des polices supprimées. Cela lui permettait de détourner les espèces. La fraude a été détectée suite à la découverte fortuite de polices supprimées avec leurs chèques encore présents dans un tiroir. Une vérification dans le système a confirmé que ces polices n'existaient plus. Cela a déclenché une mission d'audit.	Le manque de supervision de proximité, le cumul de tâches (un agent peut encaisser et comptabiliser), l'absence de vérification des suppressions dans le système, et la confiance excessive accordée à certains agents expérimentés. Par ailleurs, le fait que les agences opèrent avec un certain niveau d'autonomie peut compliquer la détection rapide des anomalies.	Garantir la fiabilité de la chaîne de traitement, depuis la souscription jusqu'à l'encaissement et la comptabilisation. Ces procédures visent également à instaurer un contrôle croisé entre les différents intervenants pour prévenir toute tentative de fraude ou de manipulation.	Chaque agence transmet un état de production ainsi qu'un état d'encaissement. Nous effectuons un rapprochement à l'échelle régionale. Si des écarts sont constatés, nous demandons des justificatifs. En parallèle, nous réalisons des audits périodiques, mais force est de constater que cela ne suffit pas toujours à détecter des fraudes élaborées.
3 : Directeur d'audit interne	La souscription est initiée en agence par le souscripteur, qui établit un projet de police sur la base des informations fournies par le client. Ce projet est validé sur l'ERP après accord du client sur les garanties et la prime. La police est ensuite imprimée, signée et transférée au caissier pour encaissement. Une fois la police validée, le caissier procède à l'encaissement selon le mode choisi : espèces, chèque, virement. L'ERP génère un avis de versement pour chaque opération. En fin de journée, les montants encaissés doivent être rapprochés de la production validée, et un état est transmis à notre direction pour contrôle et consolidation.	L'agent mis en cause, responsable de la comptabilité en agence, a profité de l'absence du souscripteur, dont la session ERP était restée ouverte, pour supprimer des polices d'assurance risques divers réglées par chèque. Il a ensuite utilisé ces chèques pour couvrir des encaissements en espèces relatifs à d'autres polices, ce qui lui a permis de détourner les espèces. La fraude a été détectée par le directeur d'agence, qui a trouvé dans un tiroir des polices supprimées avec leurs chèques. Une vérification dans le système a confirmé que ces polices n'existaient plus, et une mission d'audit interne a été	L'absence de contrôle hiérarchique immédiat, la confiance excessive envers certains agents, le cumul de fonctions (encaissement + comptabilité), et surtout la négligence dans la gestion des sessions ERP (non déconnexion, mots de passe partagés ou faibles). La faiblesse du suivi quotidien est également un facteur aggravant.	Garantir la traçabilité des flux financiers, sécuriser les fonds encaissés, et s'assurer que les encaissements correspondent bien aux polices effectivement souscrites. Elles visent aussi à prévenir les erreurs ou les détournements par une séparation stricte des tâches.	L'agence doit établir un état de production et un état d'encaissement. Ces états doivent concorder, sauf pour les ventes à crédit. Ces documents sont transmis à la direction régionale pour vérification. Néanmoins, dans la pratique, ces rapprochements sont déclaratifs et parfois superficiels. Le contrôle approfondi n'est effectué qu'en cas d'alerte.
4 : Directeur d'audit interne	Bien que ce ne soit pas directement de mon ressort, la souscription débute au niveau de l'agence, par le recueil d'informations client et la saisie des données dans l'ERP. Une fois la police validée, les documents sont transférés au caissier pour l'encaissement. Ce processus déclenche des opérations comptables que nous devons suivre. L'encaissement est effectué par le caissier sur la base des polices générées. En fin de journée, un état de caisse est dressé. Ce dernier comprend la ventilation des encaissements selon leur nature (espèces, chèques, virements). Nous générons ensuite, dans l'outil comptable, les écritures correspondantes. Toute incohérence entre les	Le mis en cause a manipulé les écritures comptables en annulant des encaissements en espèces sur des polices valides, puis en utilisant des chèques déjà encaissés pour régulariser fictivement ces opérations. Cela lui permettait de détourner les espèces. La supercherie a été découverte lorsque des polices supprimées ont été retrouvées physiquement dans un tiroir avec des chèques correspondants, ce qui ne correspondait pas aux données du système ERP. Ce décalage a déclenché un contrôle interne	Le cumul de tâches sensibles, la confiance excessive, le manque de rigueur dans la gestion des sessions ERP, et la faible fréquence des contrôles de niveau régional sur les agences. De plus, la charge de travail peut limiter la vigilance des équipes locales.	Assurer la correspondance stricte entre production et encaissement, garantir l'exhaustivité des écritures comptables, et détecter d'éventuelles anomalies ou tentatives de fraude. La traçabilité et la fiabilité de l'information financière sont au cœur de nos responsabilités.	Chaque agence doit nous transmettre l'état de production et celui des encaissements. Nous effectuons un rapprochement. Cependant, l'efficacité de ce contrôle repose sur la qualité et la sincérité des données reçues. Si une fraude est bien orchestrée en amont, il peut être difficile de la détecter immédiatement, d'où l'importance des audits inopinés.
5 : Directeur d'audit interne	La souscription se fait au niveau des agences selon un processus standardisé. Le souscripteur recueille les informations nécessaires à travers un questionnaire, établit la police via notre ERP, puis la transmet au caissier pour l'encaissement. Une fois le règlement effectué, la police est activée. Du point de vue de notre direction, nous avons pour rôle de concevoir les produits, de définir les règles de souscription, et de veiller à leur correcte application en agence. L'encaissement est réalisé par un agent habilité via un module spécifique de l'ERP. La prime peut être payée en espèces, par chèque ou autre moyen. Le paiement donne lieu à l'édition d'un avis de versement. Nous analysons régulièrement les données d'encaissement pour évaluer la performance commerciale, mais aussi pour détecter	Le fraudeur, chef de service comptabilité, a profité d'un accès inapproprié et d'une faille dans la discipline informatique pour supprimer des polices initialement payées par chèque. Il a ensuite réutilisé ces chèques pour couvrir des encaissements en espèces sur d'autres contrats, notamment auto. Cela lui permettait de détourner les espèces. L'anomalie a été découverte suite à la présence de polices supprimées (avec leurs chèques) retrouvées physiquement en agence, ce qui ne correspondait pas aux données du système.	Le cumul de fonctions, le manque de supervision, la tolérance aux dérogations, et l'absence de contrôles automatisés sont les principaux facteurs. La confiance excessive dans certains agents expérimentés, et une culture de sécurité insuffisamment ancrée, ont aussi joué un rôle dans la réalisation de cette fraude.	Assurer la conformité du processus de souscription, sécuriser les encaissements, et garantir la transparence dans le traitement des opérations. Ces procédures permettent aussi d'assurer une séparation des tâches entre la souscription, l'encaissement et la comptabilisation, ce qui est fondamental pour le contrôle interne.	Chaque agence est tenue de rapprocher l'état de production avec l'état des encaissements. Les écarts doivent être justifiés. Ces documents sont transmis à la direction régionale et centralisée pour vérification. Toutefois, ce rapprochement est manuel et repose encore trop sur la vigilance des agents, ce qui crée une zone de vulnérabilité.
6 : Directeur d'audit interne	Du point de vue informatique, cette procédure est structurée dans notre ERP, qui guide les étapes de saisie, de validation, de génération et d'impression des polices. Chaque utilisateur accède à des modules spécifiques selon son profil : souscription, modification, impression, validation, etc. L'objectif est d'encadrer strictement chaque opération par des droits d'accès individualisés. Le module d'encaissement du système ERP permet de saisir les primes perçues par mode de règlement (espèces, chèques, virements). Chaque encaissement est rattaché à une police valide et génère un avis de versement. Ces données sont ensuite intégrées dans le module comptable, ce qui permet la traçabilité des flux financiers	L'agent mis en cause a profité d'un manque de discipline dans l'usage des sessions ERP. Il a utilisé la session ouverte d'un souscripteur pour supprimer des polices initialement réglées par chèque. Ensuite, il a utilisé ces chèques pour couvrir des encaissements en espèces sur d'autres polices (automobile), détournant ainsi les espèces. La fraude a été découverte lorsqu'un directeur d'agence a retrouvé des copies papier de polices supprimées avec leurs chèques dans un tiroir. La confrontation avec le système a révélé l'écart.	Le non-respect des bonnes pratiques informatiques (partage ou oubli de déconnexion), une mauvaise gestion des habilitations, l'absence de workflow de validation pour des actions sensibles, et une tolérance à la flexibilité opérationnelle dans les agences. Tous ces éléments affaiblissent les barrières de sécurité prévues par le SI	Assurer l'intégrité des données, garantir la traçabilité des opérations, et éviter toute manipulation frauduleuse. Le système d'information doit fournir une infrastructure fiable, sécurisée et cloisonnée pour protéger l'entreprise contre les erreurs humaines ou les abus intentionnels.	Les contrôles ne sont pas centralisés automatiquement. Ils sont manuels ou semi-automatisés : les agences comparent production et encaissement, mais le système ne génère pas d'alerte sur des suppressions suspectes ou sur des incohérences entre production validée et encaissement réel. Nous manquons de tableaux de bord dynamiques à ce jour.