UCLouvain
FUCaM MONS

LOUVAIN
School of Management

Louvain School of Management

# Fraude interne : analyse, mesures de prévention et rôle de l'auditeur externe dans le processus

Auteurs : Aurélie Museur & Patricia Delpierre
Promoteur : Bénédicte Vessié
Année académique 2019-2020
Master en Sciences de gestion – Révisorat et expertise comptable

# Résumé

Une enquête menée par PricewaterhouseCoopers en 2020 intitulée « Global Economic Crime and Fraud Survey » fait état de l'importance de la fraude comptable. L'objectif de ce mémoire conjoint est d'identifier les mesures de prévention efficaces que les entreprises peuvent mettre en place afin de se protéger des risques de fraude interne. Celle-ci concerne la manipulation des états financiers et le détournement d'actifs. Nous présentons tout d'abord la fraude à l'aide de différents modèles théoriques, notamment le triangle de la fraude. Une approche théorique du contrôle interne à travers les huit composantes du modèle COSO Enterprise Risk Management (COSO ERM) est ensuite exposée. Le point suivant aborde les différents outils de prévention contre la fraude interne utilisés dans les entreprises ainsi que les différents outils de détection auxquels ont recours les auditeurs externes et réviseurs d'entreprises pour identifier le phénomène de fraude. Ensuite, sur base de la norme internationale d'audit 240, les responsabilités de l'auditeur externe dans le processus de fraude sont mises en évidence. Est ensuite présentée une étude quantitative menée auprès d'auditeurs externes et réviseurs d'entreprises dans le but d'obtenir, sur base de leur expérience, leur point de vue sur certaines situations pouvant constituer un risque de fraude, sur l'efficacité de plusieurs mesures de prévention et sur l'utilisation des outils qu'ils utilisent. Une étude qualitative réalisée auprès de réviseurs d'entreprises attachés à de grands cabinets d'audit vient affiner ces résultats. Il ressort de ces analyses que les cas de fraude sont souvent rencontrés et qu'il s'agit principalement de détournement d'actifs, qu'un environnement de travail ne tolérant aucun comportement frauduleux reste la mesure de prévention la plus efficace, mais doit être associé à d'autres mesures et que les outils d'analyse de données les plus exploités par les professionnels de l'audit sont l'analyse des ratios financiers, les arbres de décision et la loi de Benford. Enfin, un regard sur l'impact de la crise du Covid-19 dans le domaine de l'audit clôture ce travail.

Nous adressons tous nos remerciements à Madame Vessié, Professeur à l'UCLouvain FUCaM Mons et Présidente du Collège de Supervision des Réviseurs d'entreprises, notre promotrice, pour sa disponibilité, ses encouragements et ses précieux conseils tout au long de ce travail.

Nous tenons également à remercier l'ensemble de nos professeurs qui nous ont apporté des bases solides utiles pour l'exercice de notre profession future.

Enfin, nous souhaitons remercier tous les réviseurs d'entreprises et auditeurs externes qui ont bien voulu consacrer de leur temps pour répondre à nos questions.

# Table des matières

# Liste des tableaux

# Liste des illustrations

# Liste des annexes

# Introduction

Au cours de ces dernières années, bon nombre de scandales financiers ont fait la une des journaux. Les cas ayant le plus marqué les esprits sont sans aucun doute l'affaire Enron en 2001 ainsi que l'affaire Lehman Brothers en 2008.

Les entreprises, quelle que soit leur taille, ayant recours à ce genre de pratiques frauduleuses sont auditées par des cabinets, dont certains de renommée internationale, comme par exemple PricewaterhouseCoopers, KPMG, Ernst & Young ou Deloitte qui forment les Big Four. Ce fait soulève des questionnements quant à la possibilité de duper les cabinets les plus à même d'assurer la régularité des enregistrements comptables.

Bien que les scandales financiers faisant la une des journaux concernent principalement les grandes organisations, les petites entreprises ne sont pas en reste en matière de fraude ou d'agissements contraires à l'éthique.

Une enquête menée par PricewaterhouseCoopers en 2020 intitulée « Global Economic Crime and Fraud Survey » fait état de l'importance de la fraude comptable. En effet, 47 % des entreprises interrogées répondent avoir été victimes d'une fraude au cours des vingt-quatre derniers mois. Cette étude indique également que les entreprises courent un risque plus élevé de subir des dommages irréparables en cas de fraude à moins que des mesures de lutte et de prévention ne soient mises en œuvre.

Étudiantes en sciences de gestion, option révisorat et expertise comptable, à l'UCLouvain FUCaM Mons et détentrices d'un bachelier en comptabilité à la HELHa de Mons, nous avons décidé de réaliser un mémoire conjoint dont le thème porte sur l'analyse de la fraude. Ce sujet nous intéresse particulièrement dans la mesure où le réviseur d'entreprises est susceptible de rencontrer un cas de fraude au cours de l'exercice de son activité professionnelle.

L'objectif de ce mémoire est d'identifier les mesures de prévention efficaces que les entreprises peuvent mettre en place afin de se protéger des risques de fraude interne. Le rôle de l'auditeur externe dans le processus de fraude est également mis en évidence.

La thématique de la fraude n'est pas nouvelle, et dès lors la littérature nombreuse. La volonté a été de réaliser une analyse approfondie de celle-ci. Pour qu'elle soit pertinente, un nombre conséquent de sources, présentant parfois même un caractère contradictoire, ont été consultées.

Dans ce cadre, il a été utile de réaliser un mémoire à deux, à la fois pour le volume, mais également pour la discussion de ces éléments afin d'arriver, nous l'espérons, à un point de vue nuancé.

Le premier volet de ce travail présente la fraude à travers diverses statistiques récentes et différents modèles théoriques, notamment le triangle de la fraude. Nous abordons la fraude commise par des tiers, plus particulièrement celle commise au sein même de l'entreprise.

À travers la description des huit composantes du modèle COSO Enterprise Risk Management (COSO ERM), le deuxième chapitre expose une approche théorique du contrôle interne afin de déterminer si la mise en place d'un système de contrôle interne peut réellement constituer un frein aux pratiques frauduleuses.

Le troisième chapitre propose différents outils de prévention issus de la littérature pour permettre aux entreprises de se protéger des risques de fraude interne. L'objectif est de définir comment le personnel de l'entreprise devrait être contrôlé et/ou conscientisé sur l'importance d'adopter un comportement éthique. Sont également analysés dans cette partie du travail les différents outils de détection auxquels ont recours les auditeurs externes et réviseurs d'entreprises pour identifier le phénomène de fraude.

Sur base de la norme internationale d'audit 240, le chapitre suivant détaille les responsabilités de l'auditeur externe dans le processus de fraude.

Le cinquième point de ce mémoire reprend dans un premier temps les résultats d'une étude quantitative menée auprès d'auditeurs externes et réviseurs d'entreprises. Le but de cette recherche est d'obtenir, sur base de leur expérience, leur point de vue sur certaines situations pouvant constituer un risque de fraude et sur l'efficacité de plusieurs mesures de prévention. Dans un second temps, une étude qualitative a été réalisée afin d'affiner ces résultats. Il est à préciser qu'il aurait été compliqué de questionner des responsables d'entreprises et/ou leurs employés en raison de la difficulté à obtenir des informations, souvent confidentielles, sur des cas de fraude survenus au sein de ces mêmes entreprises.

Dernier point incontournable, un regard sur l'impact de la crise du Covid-19 dans le domaine de l'audit clôture ce mémoire.

Nous espérons que notre mémoire permettra d'aider les entreprises à mettre en place différents moyens de protection contre la fraude, l'intérêt étant de la prévenir le plus rapidement possible.

# Chapitre 1. La fraude

Ce premier chapitre est consacré à l'analyse de la fraude. Il est nécessaire de définir le concept de fraude et de mettre en avant des statistiques établies par de grands cabinets d'audit. Ce chapitre traite également du triangle de la fraude, du déroulement ainsi que les différents types de fraudes existants.

## 1.1. Définition et caractéristiques

Conformément aux normes d'audit internationales (ISA), la fraude se définit comme : « un acte intentionnel commis par une ou plusieurs personnes parmi les membres de la direction, les responsables de la gouvernance, les employés ou des tiers, impliquant le recours à des manœuvres trompeuses dans le but d'obtenir un avantage indu ou illégal. »

En effet, afin de distinguer une simple erreur d'un acte frauduleux, il est impératif qu'une intention de nuire soit démontrée.

La fraude est donc un concept englobant tout acte volontaire impliquant le recours à des pratiques malhonnêtes et allant à l'encontre des lois et règlements de l'organisation dans le but de détourner des biens, de la trésorerie ou encore des données confidentielles.

La réalité est que trop peu d'entreprises sont pleinement conscientes des risques de fraude auxquels elles sont confrontées. De nos jours, la lutte contre ce phénomène est devenue une activité à part entière du *core business* de l'organisation. L'époque où la fraude était considérée comme un incident isolé est bel et bien révolue.

En effet, l'échelle et l'impact de la fraude ont significativement évolué dans notre monde digital où les avancées technologiques ont permis aux fraudeurs d'utiliser des méthodes de plus en plus véreuses.

Pour la plupart des organisations, la fraude interne constitue le plus grand risque. Bien qu'il n'existe pas de méthode infaillible de prévention et de lutte contre la fraude, le risque peut être diminué en adoptant une approche systématique et réfléchie du contrôle interne.

## 1.2. Statistiques

La fraude en entreprise est un sujet souvent peu traité dans la presse pour des raisons de confidentialité. Afin de démontrer l'importance de la fraude, nous nous sommes basées sur deux études, l'une réalisée aux États-Unis et l'autre en Belgique. Nous obtenons ainsi une vision à la fois plus globale et précise de l'ampleur de la fraude.

La première étude choisie a été publiée en 2018 par l'ACFE (Association of Certified Fraud Examiners), une organisation antifraude implantée au Texas qui compte plus de 85 000 membres compétents en la matière. Sa mission consiste à réduire le risque de fraude en aidant les entreprises à la détecter et à la prévenir par la mise en œuvre de divers processus.

Son rapport, intitulé « Report to the nations : 2018 global study on occupational fraud and abuse » a été réalisé aux États-Unis et porte sur l'analyse de 2 690 cas de fraude provenant de plus de 125 pays. Étant donné que de nombreux cas de fraude ne sont pas découverts, il est difficile de déterminer le montant exact des pertes encourues. Cependant, l'étude démontre que la perte médiane pour les entreprises victimes de fraude s'élève à USD 130 000. Sur le plan mondial, la perte annuelle projetée est de 7 milliards de dollars. 89 % des cas de fraude avérés proviennent d'un détournement d'actifs, 38 % des cas incluent la corruption tandis que la manipulation des états financiers est le schéma le moins fréquent, mais entraîne des coûts considérables pour l'entreprise.

La seconde étude a été réalisée en mai 2019[1], à la demande de BDO, par un bureau de recherche externe dans le but de mesurer l'impact de la fraude au sein des entreprises belges. Cette étude a été effectuée auprès de 190 entreprises actives en Belgique. Il ressort de cette étude que 21 % des entreprises en Belgique ont été victimes de fraude au cours des cinq dernières années. De plus, tant les petites entreprises que les grandes sont victimes de fraude. Il n'existe donc pas de relation entre la taille de l'entreprise et les fraudes constatées. Par ordre d'importance, les trois types de fraude les plus fréquents sont la cybercriminalité, les déboursements frauduleux (fausses factures, travailleurs fictifs, fausses notes de frais, etc.) et les détournements d'actifs. La perte financière moyenne directe des entreprises s'élève à 200.000 EUR par fraude encourue. De plus, près de la moitié des fraudes ont été identifiées par hasard ou à la suite d'une dénonciation. D'après l'étude, la double approbation des factures et des paiements, la restriction

[1] BDO. (2019). *La fraude diminue, son coût augmente*. En ligne https://advisory.bdo.be/publications/la-fraude-diminue-son-cout-augmente/?lang=fr, consulté le 10 novembre 2019.

des accès informatiques et la formation des collaborateurs constituent les principaux moyens de prévention mis en place dans les entreprises. Des mesures de contrôle sont donc établies, mais il est impératif qu'elles soient correctement appliquées.

Ces deux études mettent en évidence l'importance du problème de la fraude. Celle-ci engendre des coûts considérables pour les entreprises qui se répercutent directement sur le bénéfice.

Nous constatons que les entreprises doivent aujourd'hui faire face à diverses menaces, notamment le vol de marchandises, la contrefaçon, la perte d'information stratégique, les cyberattaques, etc. Les entreprises prennent alors conscience de la nécessité d'investir dans la sécurité et d'instaurer des mesures de contrôle.

## 1.3. Triangle de la fraude

Le triangle de la fraude (figure 1) est un modèle expliquant les raisons qui poussent une personne à commettre une fraude professionnelle. Ce modèle a été mis au point par Donald R. Cressey (1950) grâce à plusieurs interviews réalisées dans le cadre de sa thèse de doctorat en criminologie auprès de 200 criminels incarcérés.

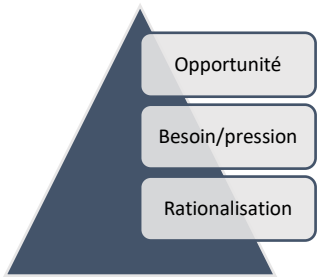



*Figure 1: Triangle de la fraude*

Les raisons de frauder varient fortement selon les individus. Ceux-ci seraient d'autant plus tentés de commettre une fraude lorsque trois facteurs sont réunis :

1) la pression ressentie par le fraudeur;

Le point de départ de toute fraude est lié à une motivation de nature économique. En général, les fraudeurs ressentent une pression financière dont ils n'osent pas parler.

Les différents types de pression rencontrés peuvent s'expliquer à travers trois aspects.

Concernant les aspects personnels, l'individu qui souhaite se mettre en avant auprès de l'employeur peut être tenté d'améliorer fictivement les résultats. À l'inverse, un individu qui désapprouve le mode de gestion de son employeur aura moins de scrupules à s'approprier des fonds de façon illégale. Le maintien d'un certain niveau de vie, la cupidité et les addictions (alcool, drogue, jeu) sont des éléments qui peuvent également amener un individu à franchir la ligne rouge.

D'un point de vue juridique, la conservation d'un contrat ou l'obtention d'un nouveau marché peuvent être à l'origine des pressions ressenties par l'individu.

Sur le plan fonctionnel, les objectifs de performance établis par l'entreprise (pressions des marchés boursiers, attentes des actionnaires) poussent l'individu à effectuer des manipulations dans les états financiers. Il est nécessaire de préciser que dans ce cas, la fraude n'est pas uniquement profitable pour la personne qui la commet.

2) l'opportunité de commettre une fraude ;

Les fraudeurs, ayant souvent une connaissance détaillée de l'entreprise, ont l'occasion de commettre un acte frauduleux en raison d'une faille dans le système de contrôle interne. En outre, le fraudeur estime que son acte sera difficilement révélé au grand jour.

Les entreprises accordent une importance particulière à ce facteur. En effet, l'occasion de commettre une fraude pourrait être évitée si l'entreprise instaure ou renforce ses mesures de contrôle.

Pour Albrecht et Zimbelman (cités dans Perrin & De Preux, 2018), les six éléments favorisant les opportunités de fraude sont les suivants :

- l'insuffisance de contrôles de prévention ou de déduction des comportements frauduleux ;
- l'incapacité à juger la qualité de la performance ;
- l'incapacité à « encadrer » les fraudeurs ;
- une lacune en matière d'accès à l'information ;
- l'ignorance, l'apathie et l'incompétence ;
- une lacune en matière de trace d'audit.

3) la rationalisation, c'est-à-dire la possibilité de justifier son acte.

Les individus se convainquent que leurs actes sont acceptables et justifiés. Chaque personne définit personnellement le caractère acceptable d'une situation. À titre d'exemple, des employés qui volent des biens de l'entreprise pourraient justifier leur acte en avançant le fait qu'ils subissent de mauvaises conditions de travail. Pour éviter cela, les entreprises mettent en place des codes d'éthique ou de déontologie.

Afin d'améliorer à la fois la prévention et la détection de la fraude, Wolfe et Hermanson (2004) proposent de rajouter un quatrième élément au triangle de la fraude, à savoir la capacité d'un individu. Ils créent alors un nouveau modèle : « le diamant de la fraude ». Ces auteurs estiment qu'une fraude se réalise s'il s'agit de la bonne personne dotée des bonnes capacités, c'est-à-dire qui transforme une opportunité de fraude en réalité.

Une personne dotée des bonnes capacités présente les caractéristiques suivantes :

1) la position ou la fonction qu'elle exerce au sein de l'organisation peut lui permettre d'exploiter une possibilité de fraude ;
2) elle est suffisamment intelligente pour comprendre et exploiter les faiblesses du contrôle interne ;
3) elle a confiance en elle et pense que son acte ne pourra pas être détecté ;
4) elle est très persuasive et peut réussir à contraindre d'autres personnes à participer à des activités frauduleuses ;
5) elle ment systématiquement pour éviter d'être démasquée ;
6) elle arrive à gérer son stress sur une longue période.

Boyle, DeZoort, et Hermanson (2015) ont évalué les effets du diamant de la fraude sur le jugement du risque de fraude par les auditeurs par rapport au modèle de base, à savoir le triangle de la fraude. L'étude révèle que les auditeurs qui utilisent le modèle du diamant de la fraude incluant la capacité d'un individu fournissent des évaluations du risque de fraude plus pertinentes. Le type de modèle de fraude utilisé affecte donc les jugements des auditeurs sur le risque de fraude.

Ces auteurs ont également observé que les effets du modèle de fraude dépendent du niveau de risque du dirigeant de l'entreprise à commettre une fraude. Le niveau de risque de fraude du PDG est élevé lorsque celui-ci est extrêmement confiant et persuasif, exerce une pression sur ses employés pour répondre aux attentes en matière de performance ou a tendance à contester les ajustements d'audit proposés. Lorsque le risque de fraude est élevé, les auditeurs qui utilisent le diamant de la fraude citent les éléments de capacité (par exemple, la capacité à gérer le stress, la capacité à tromper les autres, etc.) comme facteurs de risque importants, ce qui n'est pas le cas des auditeurs qui utilisent le triangle de la fraude.

Les deux modèles repris ci-dessus apportent une aide précieuse aux auditeurs dans l'évaluation des risques de fraude. En effet, Dowling et Leech (cités dans Boyle et al., 2015) déclarent que ces modèles améliorent la qualité de l'audit.

## 1.4. Profil du fraudeur

À titre d'illustration, une étude « Global profiles of the fraudster » réalisée par KPMG (2016) a permis d'identifier le portrait-robot du fraudeur en entreprise. Cette étude s'est basée sur 750 fraudeurs répartis dans 81 pays. Il ressort de cette analyse que près de 80 % des fraudeurs sont des hommes et 68 % des fraudeurs sont âgés de 36 à 55 ans. De plus, 65 % des fraudeurs sont des collaborateurs de l'entreprise dont 38 % travaillent dans l'organisation depuis plus de six ans et 21 % sont des anciens employés. La plupart des fraudes sont réalisées en groupe (62 %).

Cette étude permet aux entreprises d'avoir un aperçu du profil-type d'un fraudeur, même si bien sûr ce n'est qu'une information statistique.

## 1.5. Déroulement de la fraude

Alors que le triangle de la fraude a pour but d'identifier le profil du fraudeur, un autre modèle a été mis en place pour déterminer le déroulement de la fraude : le modèle du triangle de l'acte frauduleux (Kranacher et al., 2011 & Dorminey et al., 2012, cités dans Le Maux, Smaili & Ben Amar, 2013).

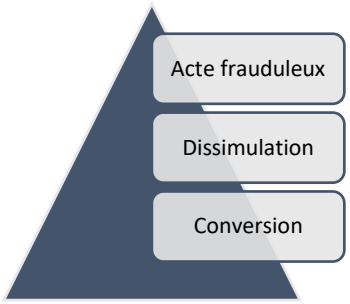



*Figure 2: Triangle de l'acte frauduleux*

Le processus de la fraude comporte cinq étapes :

1) commettre la fraude : différentes causes identifiées dans le triangle de la fraude poussent l'individu à réaliser une malversation (détournement d'actifs, vol, etc.) ;

2) cacher la fraude : après avoir commis une fraude, le fraudeur fera tout pour dissimuler son acte (fausses écritures comptables, destruction de fichiers informatiques, etc.) ;

3) convertir les éléments en un avantage utilisable : l'objectif du fraudeur est de transformer des éléments non monétaires en espèces facilement utilisables et négociables (détournement de chèque) ou encore convertir des bénéfices acquis illégalement en des actifs utilisables (blanchiment d'argent).

Les trois premières phases se rapportent directement au fraudeur. Perrin et De Preux (2018) ajoutent deux étapes qui concernent le forensic accountant ou la victime de fraude :

4) chercher les symptômes de la fraude : lorsque la fraude est constatée, la victime ou les investigateurs mèneront diverses actions pour découvrir l'origine de la fraude et obtenir des preuves ;

5) contrôler : l'entreprise devra définir des mesures de contrôle afin d'éviter que ces actes se reproduisent à l'avenir.

L'examen des différentes étapes de l'acte frauduleux permet à l'entreprise de mettre en place les moyens nécessaires pour lutter contre la fraude.

## 1.6. Types de fraude

Afin de survivre dans un environnement de plus en plus concurrentiel, de nombreuses entreprises ont jugé nécessaire de trouver des alliances et de constituer un groupe de taille suffisante grâce à la création de filiales étrangères. Dès lors, il est évident que plus le réseau de l'entreprise s'agrandit hors de son pays d'origine, plus celui-ci devient complexe et risqué.

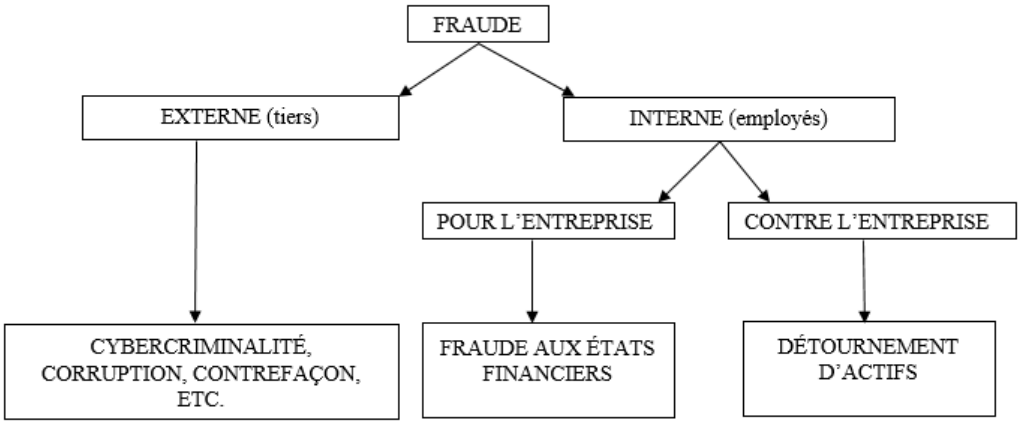



*Figure 3: Catégories de fraude*

Ce point illustre deux grands types de fraudes: la fraude commise par des tiers et celle commise par des employés (figure 3).

### 1.6.1. Fraude externe

À l'heure actuelle, les différentes parties prenantes (clients, salariés, fournisseurs, actionnaires, consommateurs, etc.) ressentent le besoin d'être rassurés. Bien connu pour sa théorie de la motivation, Abraham Maslow affirme que chaque être humain a des besoins qu'il doit satisfaire. Il effectue ainsi une hiérarchisation des besoins fondamentaux. Il apparaît que le besoin de sûreté et de sécurité arrive juste après les besoins physiologiques. Cette théorie prouve l'importance pour les parties prenantes d'évoluer dans un environnement sécurisé. Pourtant, les entreprises sont susceptibles de subir diverses menaces d'origine externe.

#### *1.6.1.1. Espionnage industriel*

L'espionnage industriel consiste à voler de l'information auprès des entreprises concurrentes. Ce phénomène connaît une phase de croissance en raison du développement des Nouvelles Technologies de l'Information et de la Communication (NTIC). Il est important de signaler que la perte d'informations peut également provenir d'un manque de vigilance de la part de personnes chargées de conserver ces informations. Toute information susceptible de nuire au développement de l'entreprise doit faire l'objet d'une attention particulière et des mesures de protection doivent être envisagées (Hassid & Masraff, 2010).

#### *1.6.1.2. Contrefaçon*

L'essor d'internet permet à n'importe qui de se procurer des produits contrefaits. Il ressort d'un article (Gomez, 2017) qu'au niveau européen, 41 millions de produits ont été saisis en 2015, représentant une valeur de 642 millions d'euros. Sans surprise, la Chine est souvent à l'origine de ces articles contrefaits. Ce phénomène touche principalement l'industrie du luxe ainsi que le secteur pharmaceutique, bien que les produits de grande consommation sont également aujourd'hui visés. Afin de combattre la contrefaçon, les entreprises doivent se faire aider par les autorités locales pour fermer les sites illégaux et porter plainte contre ces sociétés frauduleuses.

#### *1.6.1.3. Cybercriminalité*

Les systèmes informatiques deviennent indispensables pour gérer une entreprise au quotidien (stockage des données, outil de communication, e-commerce, etc.). Les entreprises sont donc plus vulnérables au risque de cybercriminalité dont le but est de voler des informations stratégiques grâce à des virus et des logiciels espions. Le turn-over dans les entreprises, la sous-traitance, les voyages d'affaires accentuent la diffusion d'informations et de ce fait, le piratage informatique. Pour faire face à ce phénomène, les entreprises doivent sécuriser les systèmes informatiques en garantissant l'authentification des utilisateurs. Les technologies évoluant rapidement, les entreprises doivent constamment réviser leurs installations pour assurer un certain niveau de sécurité (Hassid & Masraff, 2010).

L'Europe tente de lutter contre les logiciels pirates. Une méthode utilisée par les fraudeurs pour s'attaquer à l'ensemble du monde virtuel est le rançongiciel, apparu en 1989. Il s'agit d'un programme malveillant inséré dans un mail ou directement proposé sur internet. Une fois le programme ouvert, celui-ci verrouille l'ordinateur en exigeant un paiement pour rétablir l'accès aux données. Un rançongiciel connu, « Wann Cry », a touché plus de 150 pays en mai 2017, dont notamment la Belgique. Une entreprise confrontée à ce genre de situation doit avant tout déconnecter toutes les machines reliées à l'ordinateur (clé USB, disque dur externe, etc.) ainsi que le réseau internet pour éviter la propagation du virus[2].

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) participent collectivement et de manière complémentaire à l'élaboration des Normes internationales. Parmi celles-ci, la famille des normes ISO 27000 peut aider les organisations à garantir la confidentialité de leurs informations stratégiques (données financières, documents soumis à la propriété intellectuelle, informations relatives au personnel, etc.). Plus précisément, la norme internationale ISO/CEI 27001 : 2013 spécifie les exigences relatives au développement d'un système de management de la sécurité de l'information (SMSI) au sein des entreprises. Chaque organisation doit ensuite adapter constamment son système de gestion de la sécurité informatique en fonction de ses objectifs, de sa taille et de sa structure.

[2] DH.be. (2019). *Cybercriminalité : l'Europe lutte contre les logiciels pirates*. En ligne https://www.dhnet.be/actu/new-tech/cybercriminalite-l-europe-lutte-contre-les-logiciels-pirates-5c9b83b87b50a60b4559a03a, consulté le 27 août 2019.

#### *1.6.1.4. Fraude au président*

La fraude au président ou la fraude au CEO (Chief Executive Officer) est relativement récente et très dangereuse pour l'entreprise. Ce type de fraude repose sur une bonne connaissance de l'entreprise en matière d'organigramme et d'emploi du jargon interne à celle-ci.

Tout d'abord, l'auteur de la fraude procède à une étude approfondie de l'organisation et de son top management en récoltant des informations sur l'organigramme de la société et via les réseaux sociaux.

Ensuite, l'auteur se fait passer pour le dirigeant de l'entreprise et sous le prétexte d'une opération urgente et confidentielle demande une transaction financière rapide. Bien souvent l'employé visé s'exécute en toute confiance sans préalablement effectuer de vérifications. À titre d'exemple, un groupe belge[3] spécialisé dans les spiritueux a subi un dommage de 800.000 EUR en 2015 avec une fraude au président.

Pour se protéger de ce type de fraude, les entreprises doivent être conscientes de ce risque. Elles doivent notamment mettre en place des procédures strictes avant d'autoriser un paiement.

#### *1.6.1.5. Attaques informationnelles*

Une entreprise peut être victime d'accusations rendues publiques, d'informations mensongères diffusées par les médias, ternissant ainsi son image de marque. Dans le but d'influencer l'opinion publique, de faux communiqués de presse peuvent être publiés pour faire chuter le cours de l'action. Les conséquences de ces attaques informationnelles peuvent être considérables. En effet, une dégradation de l'image de marque impacte négativement l'activité commerciale, d'autant plus si le développement de l'entreprise est basé sur son image de marque. Les clients se détournent du produit et les travailleurs au sein de l'entreprise sont démotivés à l'idée de faire partie d'une entreprise dont l'image est ternie.

Les entreprises peuvent également être touchées par les appels à boycott. Le boycott se définit comme étant « une protestation organisée, où un groupe décide de politiser l'acte de non-achat en diffusant sa consigne auprès du grand public » (Hassid & Masraff, 2010).

[3] RTBF info. (2017). *La « fraude au CEO », ou comment les escrocs arrivent à se faire passer pour le président*.

Face à ces menaces, les entreprises doivent développer une communication active, c'est-à-dire faire en sorte que les interlocuteurs se sentent entendus et compris.

### *1.6.1.6. Corruption*

Transparency International définit la corruption comme étant : « l'abus de pouvoir reçu en délégation à des fins privées ».

De nos jours, la corruption demeure un problème auquel les entreprises doivent faire face. En effet, contrairement aux idées préconçues, la corruption ne touche pas uniquement des pays en voie de développement. Celle-ci peut revêtir différentes formes dans nos contrées telles que les conflits d'intérêts, les sponsorships douteux, etc.

Une étude menée par Deloitte, un des quatre plus importants cabinets d'audit dans le monde, indique les différentes formes que peut prendre cette problématique (figure 4).

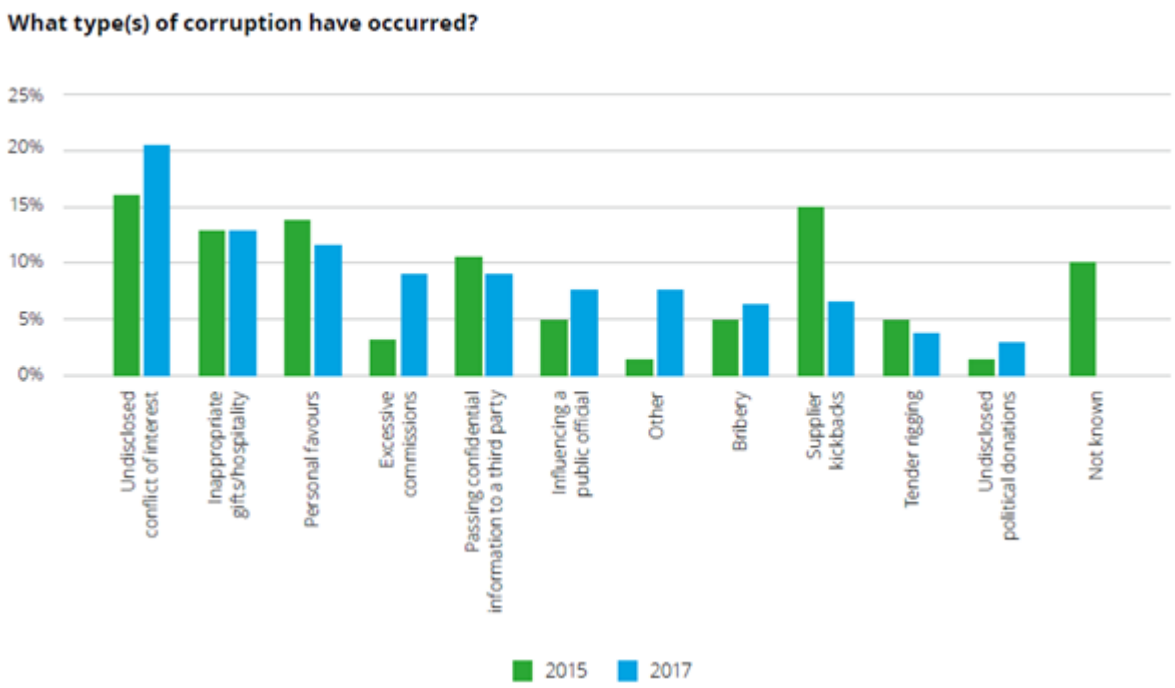



*Figure 4: Bribery and corruption survey report 2017 - Deloitte*

Perrin et De Preux (2018) identifient les trois principaux types de la corruption, à savoir les pots-de-vin, les ententes illégales et les conflits d'intérêts.

Selon eux, le pot-de-vin est une transaction illégale et non éthique par laquelle on « achète » l'influence du bénéficiaire. Dans la plupart des cas, le fournisseur effectue un paiement auprès d'un employé de l'acheteur dans le but d'obtenir un marché. Un employé qui dispose d'un pouvoir de décision important pourrait également être tenté de vendre des marchandises à un prix inférieur et recevoir en retour un pot-de-vin.

Les ententes illégales peuvent prendre la forme de cartels ou de soumissions concertées. Ces dernières consistent à créer un groupe d'offreurs qui se mettent d'accord sur un prix à proposer pour un marché public donné.

Il n'est pas évident de mesurer l'impact des conflits d'intérêts au sein des entreprises. Afin de prévenir les conflits d'intérêts, les employés (chargés de la gestion des achats, des investissements ou de la négociation des contrats) devraient déclarer à leur employeur des éléments relatifs à leur situation personnelle ou les éventuels conflits d'intérêts qui pourraient survenir dans l'exercice de leurs fonctions.

La corruption peut gravement nuire aux personnes impliquées, mais aussi à l'organisation dans son ensemble et bien souvent sur le long terme. Il est important de préciser que la corruption est plus difficile à prouver que le détournement d'actifs ou la fraude aux états financiers, car la corruption ne se concrétise quasiment pas au travers de la comptabilité (Perrin & De Preux, 2018).

Depuis de nombreuses années, des réglementations globales ont visé à atténuer les effets de la corruption sur les marchés. Cependant, le risque reste présent et demeure une préoccupation pour bon nombre d'entreprises. Selon un sondage mené par PwC[4], près de 30 % des organisations interrogées reconnaissent ce risque.

Une étude menée par Ernst & Young, quant à elle, montre que 40 % des sociétés interrogées dans le cadre de ce sondage indiquent que la corruption est amplement répandue et demeure une menace de taille.

[4] PwC. (2020). *Fighting fraud: A never-ending battle. PwC's Global economic crime and fraud survey*. En ligne https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf, consulté le 9 mai 2020.

Dans un contexte de marchés en expansion, d'une législation plus large et de pressions financières mondiales, les impacts de la corruption peuvent avoir une grande portée et peuvent inclure :

- des condamnations, amendes et peines de prison pour les employés et les dirigeants ;
- des honoraires juridiques substantiels, y compris en coût de conformité ;
- des dommages importants à la réputation de l'entreprise ;
- une détérioration du cours de l'action et une perte de confiance des actionnaires et des autres parties prenantes ;
- une distorsion du marché.

La plupart des organisations disposent d'un code de conduite et d'une formation pour les nouveaux employés ainsi que d'une politique et des procédures de gestion relatives à des fonctions importantes telles que les achats et le marketing. Ces mesures constituent donc une réponse à cette problématique.

Si l'organisation ne dispose pas déjà d'un code éthique ou d'un code de conduite, celui-ci doit être créé. Ces codes doivent s'attaquer à la corruption ainsi qu'à d'autres questions liées à l'éthique commerciale générale.

Les codes existants doivent être examinés et mis à jour si besoin afin de garantir que les aspects liés à la lutte contre la corruption soient correctement pris en compte. Tous les codes doivent être approuvés par le conseil d'administration et refléter les valeurs fondamentales que l'organisation cherche à implémenter. Ces codes fournissent donc des directives spécifiques à la direction et au personnel.

Il existe un certain nombre de directives relatives à la lutte contre la corruption, notamment des mesures en matière d'/de:

- intermédiaires et autres partenaires commerciaux ;
- cadeaux et divertissements ;
- dons caritatifs ou politiques, activité de lobbying ;
- conflits d'intérêts ;
- comptes bancaires, caisse.

Selon une étude spécifique à cette problématique menée par PwC[5], il n'est ni nécessaire ni réaliste que ces mesures s'efforcent de traiter tous les cas de figure possibles où un acte de corruption pourrait être posé. Il est préférable de développer et d'intégrer clairement les valeurs que l'entreprise s'efforce de véhiculer afin que les employés puissent être guidés dans le processus de prise de décision éthique. C'est pourquoi ces procédures et contrôles anticorruption doivent être intégrés dans les procédures opérationnelles et de contrôle interne de l'entreprise.

Les meilleures pratiques en matière de lutte contre la corruption exigent généralement la mise en place de mécanismes permettant de signaler de manière confidentielle et anonyme tout soupçon de corruption.

### 1.6.2. Fraude interne

Sutherland (1883-1980), sociologue américain, a inventé l'expression de *crime à col blanc*, c'est-à-dire des crimes causés par des cadres ou des dirigeants d'entreprises. À l'heure actuelle, les fraudes sont commises par des personnes qui proviennent de n'importe quel milieu social.

#### *1.6.2.1. Détournement d'actifs*

Les entreprises prévoient des mesures contre les menaces extérieures, mais elles doivent également penser aux risques internes qu'elles encourent.

L'Association of Certified Fraud Examiners (ACFE) définit la fraude interne, aussi appelée *occupational fraud*, comme étant « the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets ».

Les détournements d'actifs peuvent être réalisés tant par des employés que des dirigeants.

L'étude réalisée par BDO (cfr page 4) a montré que 45 % des fraudes sont commises par du personnel de l'entreprise.

Perrin et De Preux (2018) identifient, sur base du manuel établi par l'ACFE, les différentes catégories de détournements d'actifs. Les employés peuvent s'enrichir personnellement, au

[5] PwC. (2016). *Assessing the risk of bribery to your business.*
En ligne https://www.pwc.com.au/pdf/assessing-the-risk-of-bribery-and-corruption-oct2016.pdf, consulté le 12 novembre 2018.

préjudice de la société, de diverses façons. Ils peuvent tout simplement voler de l'argent dans la caisse ou encore empocher l'argent d'une vente au comptant sans enregistrer l'opération comptable (écrémage). Dans ce dernier cas, la marge brute ainsi que le chiffre d'affaires se trouvent directement affectés. Évidemment, les employés peuvent également tirer profit de biens détournés de l'entreprise. Ces biens seront soit utilisés à des fins privées par le fraudeur, soit revendus à des tiers.

Un autre type de fraude consiste à envoyer de fausses factures à l'aide d'un nom, d'une adresse et d'un compte bancaire modifié. Cette fraude est souvent commise par des employés qui ont un accès direct à la comptabilité de l'entreprise ou qui s'occupent de la gestion des paiements. Dans la plupart des cas, les factures concernent des prestations de services, plus difficiles à déceler, étant donné que l'achat de marchandises requiert des procédures de réception et de stockage plus spécifiques.

Une entreprise peut également se retrouver à payer des salaires sans se douter qu'elle paie pour un employé fictif ou un employé qui n'est plus présent dans l'entreprise. En modifiant le numéro de compte bancaire, le fraudeur profite donc d'un salaire payé indûment. Il est à noter que cette situation se présente plutôt dans des entreprises qui comptent beaucoup d'employés.

Lorsque les employés demandent un remboursement de leurs frais professionnels (frais de voyage, frais d'hôtel, etc.), ceux-ci peuvent être tentés d'effectuer diverses manipulations. En effet, les employés pourraient demander le remboursement de frais qui ne sont pas liés à l'activité professionnelle, gonfler le montant des dépenses ou encore créer des frais fictifs à l'aide de faux documents. La fraude au remboursement de frais est assez fréquente, mais il est possible de la détecter facilement en analysant l'évolution des comptes de charges par rapport aux années précédentes. De plus, plusieurs informations (date, montant, lieu) doivent faire l'objet d'un contrôle afin de vérifier que les dépenses engagées correspondent à l'objet de la mission.

En général, les détournements d'actifs sont effectués par les employés. Cependant, les dirigeants peuvent également dilapider les ressources de l'entreprise. Ils peuvent par exemple mettre un véhicule de la société à disposition de leur conjoint ou encore effectuer des travaux dans leur résidence principale. Ces détournements peuvent prendre une forme plus complexe comme la dissimulation des avoirs dans des filiales étrangères. Ces actes frauduleux sont

souvent associés à des manipulations dans les écritures comptables afin d'éliminer toutes les preuves.

Nous constatons que ce ne sont pas les occasions qui manquent pour commettre une fraude interne. Les entreprises confrontées à ce genre de situations ne disposent pas de contrôles effectifs, offrant ainsi une opportunité de détournement d'actifs.

De plus, le concept de management override se répand de plus en plus. Les procédures de contrôle interne sont les garanties mises en place par les entreprises afin de protéger leurs ressources financières contre la fraude et les différents abus[6]. C'est donc dans cet objectif que la direction est responsable de l'application de ce contrôle interne auprès des employés.

Bien évidemment, la bonne application du contrôle interne est opérée par un organe de contrôle au sein de l'organisation. Cependant, dans certains cas, les contrôleurs peuvent penser qu'ils ont la capacité d'opérer en dehors des règles de contrôle interne préétablies afin de se procurer un avantage personnel au détriment de la société.

Il existe trois types de situations spécifiques de management override :

- antidater les documents financiers ;
- procéder à des ajustements des écritures comptables durant le processus de clôture de l'exercice ;
- manipuler les informations quant à la santé financière de l'entreprise.

Le management override relatif au contrôle interne peut constituer une violation majeure des politiques comptables d'une organisation.

La détection de ce type de fraude s'avère être particulièrement ardue. Bon nombre de compagnies attribuent une fonction de contrôle aux différents managers afin de vérifier le travail effectué par un employé. Il est donc compliqué de détecter un management override du fait de la position hiérarchique et stratégique de son auteur.

[6] Vitez, O. (2019). *What is management override of internal controls ?* En ligne https://bizfluent.com/facts-6052778-management-override-internal-controls-.html, consulté le 12 novembre 2019.

En effet, ce dernier maîtrise les différents outils de contrôle et bien souvent met en place les procédures de contrôle interne pour l'entreprise. Ceci lui laisse donc une certaine liberté d'action dans un éventuel processus d'élaboration de fraude.

Cependant, certaines mesures peuvent être adoptées afin de prévenir ou contenir le phénomène.

Dans cette optique, l'entreprise concernée mettra en œuvre des audits internes et externes afin d'examiner ses informations financières. Ces audits permettent d'avoir une vision objective sur la manière dont la politique comptable est appliquée au sein de l'organisation.

#### *1.6.2.2. Manipulation des états financiers*

La manipulation des états financiers est une fraude interne à l'entreprise, commise à son avantage. Selon Perrin & De Preux (2018), cette fraude se définit comme l'utilisation de la comptabilité et des rapports financiers de manière arbitraire et de façon à modifier, à la hausse ou à la baisse, les résultats financiers.

L'étude de BDO (cfr page 4) révèle que la falsification des états financiers ne représente que 2 % des fraudes subies. De plus, l'étude réalisée par l'Association of Certified Fraud Examiners en 2018 (cfr page 4) démontre que les cas de fraude aux états financiers ne sont pas les plus nombreux, mais sont à l'origine des pertes les plus importantes par rapport aux autres cas étudiés précédemment (figure 5).


*Figure 5: How is occupational fraud committed? (ACFE, 10)*

Les actionnaires, les banquiers ou encore le personnel ont tous des attentes spécifiques en ce qui concerne le résultat. Mohamed et Handley-Schachler (2015) mettent en lumière différentes théories en identifiant les raisons qui concourent à l'établissement d'états financiers frauduleux.

La théorie de l'agence décrit les relations contractuelles qui existent entre le principal (à savoir les actionnaires) et l'agent (à savoir les dirigeants). Le but de cette théorie est de faire en sorte que les intérêts des dirigeants soient conformes aux intérêts des actionnaires en sachant que chaque individu cherche à maximiser son utilité. L'agent accomplit une tâche au nom et dans l'intérêt du principal. D'un côté, la direction doit fournir des états financiers fiables aux actionnaires afin de réduire le risque d'agence[7]. D'un autre côté, les actionnaires, en tant que propriétaires de la société, apportent le capital et supportent les risques de l'entreprise. La théorie de l'agence met en évidence une des raisons qui peut pousser les dirigeants à manipuler les états financiers. En effet, pour respecter leurs obligations envers les actionnaires, les dirigeants peuvent être tentés de dissimuler des performances médiocres en surestimant les revenus et les actifs ou en sous-estimant les dépenses et les dettes.

La théorie des parties prenantes vise à prendre en compte les préoccupations de l'ensemble des parties prenantes de l'entreprise (actionnaires, employés, banque, etc.). Dans cette optique, chacune d'entre elles a ses propres intérêts et tente de manipuler les états financiers à son avantage. Les cadres supérieurs sont souvent les mieux placés pour manipuler les états financiers au détriment des actionnaires.

La théorie de l'intérêt public signifie que l'entreprise a également une responsabilité envers la société en général. La fraude aux états financiers peut consister à maquiller le montant des impôts à payer en dissimulant des bénéfices excédentaires.

La théorie des besoins en capital consiste à conserver les investisseurs existants ou à attirer d'autres investisseurs pour lever des fonds. Dans certains cas, la fraude aux états financiers est utilisée pour manipuler les actionnaires, par exemple en gonflant temporairement les bénéfices. Les cadres supérieurs peuvent également faire en sorte d'augmenter le prix de l'action lorsqu'ils vendent et le baisser lorsqu'ils achètent.

La théorie de la communication vise à améliorer la diffusion des informations financières aux utilisateurs des comptes. L'efficacité de cette diffusion est garantie grâce à un contrôle du

[7] Le risque d'agence représente le risque que le résultat de l'action de l'agent pour le principal diffère fortement du résultat attendu en cas de maximisation effective des intérêts du principal.

processus de production des états financiers. Pour rappel, la publication d'informations financières fiables reflétant l'activité réelle de l'entreprise incombe à la direction. Le fait de dissimuler ou de transmettre des informations erronées aux lecteurs des comptes fait partie d'une catégorie de fraude aux états financiers.

Il y a lieu d'ajouter que l'enregistrement des charges et des produits dans une mauvaise période comptable constitue également une fraude aux états financiers. Dans ce cas, la fraude consiste à améliorer le bénéfice par l'augmentation des produits (anticipation des recettes) ou par la diminution des charges (report des dépenses sur l'exercice suivant).

Notons que la norme ISA 315 stipule que la reconnaissance des revenus constitue en soi un risque de fraude, sauf justification contraire. Cette problématique est un concept à ce point crucial que le cadre normatif comptable est en évolution constante. Ainsi, en mai 2014, le FASB (Financial Accounting Standards Board) et l'IASB (International Accounting Standards Board) ont mené un projet conjoint qui a abouti à une mise à jour de la norme traitant du moment et de la manière dont les produits sont constatés. Il s'agit de la norme IFRS 15. Cette norme comporte un principe de base qui, pour illustrer le transfert de biens ou de services promis aux clients, stipule qu'une entité doit comptabiliser les produits d'un montant qui reflète la contrepartie à laquelle l'entité s'attend à avoir droit en échange de ces biens ou services.

La reconnaissance des revenus peut être résumée en cinq étapes :

- identifier le contrat avec le client ;
- identifier les obligations de performance dans le contrat ;
- déterminer le prix de la transaction ;
- allouer le prix de la transaction aux obligations de performance ;
- reconnaître le revenu quand l'entité satisfait les obligations de performance.

Cette norme prévoit également une augmentation des informations à fournir, donnant ainsi aux utilisateurs des états financiers des renseignements complets sur la nature, le montant, le calendrier et l'incertitude des revenus et des flux de trésorerie résultant des contrats avec les clients.

La fraude relative à la reconnaissance des revenus est au centre des préoccupations, en grande partie surtout parce que les revenus sont une catégorie principale qui affecte la situation financière et les résultats d'exploitation d'une entité.

En outre, comme mentionné précédemment, la direction peut être tentée de gonfler les revenus, car les primes versées sont souvent déterminées par ceux-ci. La manipulation des revenus pourrait entraîner des anomalies au niveau de l'EBITDA d'une entité et d'autres ratios de rentabilité sur lesquels les investisseurs et le public comptent pour prendre des décisions d'investissement. Le recours à cette pratique pourrait aussi déformer le cours de l'action.

La norme ISA 315, révisée en 2019, est particulièrement pertinente dans ce contexte, car, d'une certaine manière, elle transpose ces concepts dans le cadre de l'audit. En effet, elle prévoit que l'auditeur doit acquérir une compréhension de l'entité et de son environnement, y compris de son contrôle interne, suffisante pour identifier et évaluer les risques d'anomalies significatives dans les états financiers provenant d'une fraude ou d'une erreur, et suffisante pour concevoir et exécuter d'autres procédures d'audit.

Pour ce faire, l'auditeur doit procéder à une évaluation des risques au niveau des états financiers et des assertions sur base d'une compréhension appropriée de l'entité.

Cette norme rappelle qu'elle doit être appliquée conjointement aux directives fournies par d'autres normes ISA et tout particulièrement la norme ISA 240 relative à la fraude.

Une étude réalisée par l'organisme COSO[8] sur 347 cas de fraude dans des états financiers a révélé que les mécanismes inappropriés de reconnaissance de revenus représentaient 61 % des cas.

[8] COSO. (2010). *Fraudulent financial reporting 1998-2007*. En ligne https://www.coso.org/Documents/COSO-Fraud-Study-2010-001.pdf, consulté le 6 avril 2020.

# Chapitre 2. Environnement du système de contrôle interne

Avant que de nombreux scandales financiers n'éclatent, la prévention de la fraude ne constituait pas l'objectif principal du système de contrôle interne d'une entreprise.

Aujourd'hui, la fraude fait partie des risques les plus importants auxquels les investisseurs sont devenus plus sensibles. En effet, les pertes collatérales générées par une fraude, notamment la réputation de l'entreprise, peuvent s'avérer plus conséquentes que les pertes financières directes. Lorsqu'une fraude est détectée, la confiance entre les investisseurs et la direction est rompue. C'est pourquoi les investisseurs accordent une importance particulière au contrôle interne et à l'audit interne en tant qu'éléments essentiels des systèmes de prévention et de détection de la fraude (Petraşcua & Tieanu, 2014).

## 2.1. Présentation du référentiel COSO

Ce point présente les deux cadres du COSO : le modèle COSO Internal Control (COSO IC) et le modèle COSO Enterprise Risk Management (COSO ERM).

Le référentiel COSO est le cadre le plus largement répandu dans les domaines du contrôle interne et de la gestion des risques d'entreprise.

COSO est une organisation fournissant un « leadership éclairé et des conseils sur le contrôle interne, la gestion des risques et la lutte contre la fraude » (Protiviti, 2014).

Il reprend des lignes directrices relatives à des procédures de contrôle interne sur lesquelles la direction de l'entreprise peut se baser. Il est conçu en vue de soutenir des objectifs tels que : protéger les actifs, encourager les employés à respecter la politique de l'entreprise, garantir un enregistrement comptable précis et fiable en se conformant aux exigences légales.

La première version du COSO a été introduite en 1992 et est rapidement devenue prédominante en matière de contrôle interne suite à l'adoption de la loi Sarbanes-Oxley en 2002 par le congrès américain suite à plusieurs scandales comptables et financiers. Depuis lors, le référentiel a été mis à jour en 2013 en y intégrant une perspective de gestion des risques (figure 6).


*Figure 6: COSO 2013 (Protiviti 2014, 2)*

Le COSO IC dispose de cinq composantes : environnement de contrôle, évaluation des risques, activités de contrôle, information et communication et pilotage. Ces cinq composantes intègrent 17 principes[9].

Le COSO ERM fut créé en réponse au manque criant de littérature commune relative au risque et à la gestion du risque. Il était nécessaire d'examiner le risque au niveau de l'entreprise dans son ensemble. De ce fait, ce référentiel est bien plus large que le COSO IC.

Selon COSO, la définition de l' « Enterprise Risk Management » est :

> un processus mis en œuvre par le conseil d'administration, les directeurs et les membres du personnel, appliqué dans l'élaboration des stratégies et au travers de toute entité et activités de l'entreprise. Il a été conçu pour identifier tout événement potentiel susceptible d'affecter l'entité, pour s'assurer que le risque entre dans les limites du « risk appetite » de l'entité et pour fournir une assurance raisonnable concernant la réalisation de ses objectifs. (Cours de contrôle interne et gestion des risques, 2018)

[9] Cfr annexe 1 : Les 17 principes du référentiel COSO, page A1

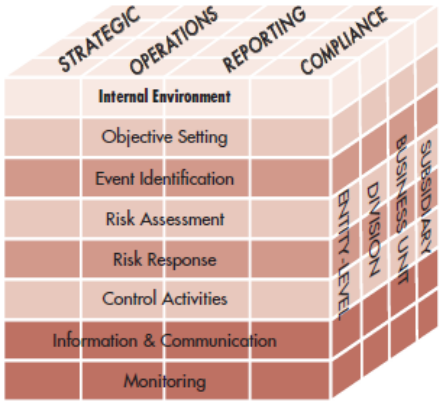



*Figure 7: COSO ERM (Romney & Steinbart 2016, 204)*

Nous constatons que le champ d'application du COSO ERM (figure 7) est plus vaste que son prédécesseur avec huit composantes dont la dénomination a été quelque peu modifiée :

- environnement interne ;
- **fixation des objectifs** ;
- **identification des événements** ;
- évaluation des risques ;
- **réponse aux risques** ;
- activités de contrôle ;
- information et communication ;
- surveillance.

Le cadre IC a été largement adopté comme moyen d'évaluer les contrôles internes, comme l'exige la loi Sarbanes-Oxley.

Le cadre ERM, plus complet, adopte une approche basée sur les risques plutôt qu'une approche basée sur les contrôles. L'ERM ajoute trois éléments supplémentaires au cadre du COSO IC : fixer des objectifs, identifier les événements susceptibles d'affecter l'entreprise et élaborer une réponse aux risques évalués. Les contrôles sont donc flexibles et pertinents car ils sont liés aux objectifs organisationnels. Le modèle ERM reconnaît également que le risque, en plus d'être maîtrisé, peut être accepté, évité, diversifié, partagé ou transféré.

## 2.2. Composantes du COSO ERM

Parce qu'il est plus complet, le modèle ERM est ici analysé pour expliquer les contrôles internes. En effet, si le modèle ERM est bien assimilé, il est aisé de comprendre le modèle IC qui repose sur cinq des huit composantes du modèle ERM.

### 2.2.1. Environnement interne

L'environnement interne, ou la culture d'entreprise, influence la façon dont les organisations établissent des stratégies et des objectifs, structurent les activités commerciales et identifient, évaluent et répondent au risque. Il est le fondement de toutes les autres composantes du COSO ERM. Un environnement interne faible ou déficient entraîne souvent des défaillances dans la gestion et le contrôle des risques.

Un environnement interne se compose des éléments suivants:

- philosophie de la direction, style de fonctionnement et goût du risque ;
- engagement en matière d'intégrité, de valeurs éthiques et compétence ;
- surveillance du contrôle interne par le conseil d'administration ;
- structure organisationnelle ;
- méthodes d'attribution de l'autorité et de la responsabilité ;
- normes de ressources humaines qui attirent, développent et retiennent des personnes compétentes ;
- influences extérieures.

### 2.2.2. Fixation des objectifs

La définition des objectifs est le deuxième composant du modèle ERM. La direction détermine ce que l'entreprise espère atteindre, souvent appelé la vision ou la mission de l'entreprise. La direction fixe des objectifs au niveau organisationnel, puis les subdivise en objectifs plus spécifiques pour les sous-unités de l'entreprise.

L’entreprise détermine la marche à suivre pour atteindre les objectifs et établit des mesures d’évaluation de la performance pour déterminer si elles sont respectées.

Les objectifs stratégiques sont des objectifs de haut niveau alignés sur la mission pour soutenir et créer de la valeur pour les actionnaires. Ils sont définis en premier. La direction doit identifier les moyens d'atteindre les objectifs stratégiques en identifiant et évaluant les risques et implications de chaque alternative. Elle doit ensuite formuler une stratégie d'entreprise et fixer des objectifs d'exploitation, de conformité et de rapport.

Les objectifs opérationnels portent sur l'efficacité et l'efficience des opérations de l'entreprise et déterminent la manière d'allouer les ressources. Ils reflètent les préférences, les jugements et le style de gestion et sont un facteur clé du succès de l'entreprise.

Les objectifs de conformité aident l'entreprise à se conformer à toutes les lois et réglementations applicables.

Les objectifs de reporting aident à garantir l'exactitude, l'exhaustivité et la fiabilité des rapports établis par l'entreprise. Ils permettent d'améliorer la prise de décision et de surveiller les activités et les performances de l'entreprise.

La plupart des objectifs de conformité et de reporting sont imposés par des organismes normatifs en réponse aux lois ou règlements. Le modèle ERM fournit une assurance raisonnable que ces deux objectifs sont atteints car les entreprises ont établi un contrôle de ceux-ci.

Cependant, en termes d'objectifs stratégiques et opérationnels, l'assurance que fournit le modèle ERM n'est que limitée. En effet, ces objectifs sont bien souvent tributaires d'événements externes incontrôlables.

### 2.2.3. Identification des événements

COSO définit un événement comme étant « un incident ou un événement émanant de sources internes ou externes affectant la mise en œuvre de la stratégie ou la réalisation des objectifs. Les événements peuvent avoir un impact positif ou négatif ou les deux ».

Un événement positif représente une opportunité tandis qu'un événement négatif représente un risque. Il s'agit donc d'une forme d'incertitude, cela peut se produire ou pas. Il est difficile de savoir quand un évènement va se produire et de déterminer son impact a priori. Cela peut aussi déclencher un autre événement. De ce fait, les événements peuvent se produire individuellement ou simultanément.

La direction doit donc essayer d’anticiper tous les événements positifs ou négatifs possibles, déterminer lesquels sont le plus ou le moins susceptibles de se produire et comprendre l'interrelation des événements.

Certaines techniques utilisées par les entreprises pour identifier les événements incluent l'utilisation d'une liste complète des événements potentiels, la réalisation d'une analyse interne, le suivi des événements principaux et des points de déclenchement, etc.

### 2.2.4. Évaluation et réponse aux risques

Hassid et Masraff (2010) déclarent que les entreprises intelligentes, créatrices de valeur, savent pertinemment qu’il n’y a pas d’opportunité sans risque.

La direction doit spécifier clairement ses objectifs afin de pouvoir identifier et évaluer les risques auxquels elle pourrait être confrontée dans le cadre de ses activités. Comme indiqué précédemment, cela devrait inclure une évaluation de toutes les menaces, y compris les catastrophes naturelles et politiques, les erreurs logicielles, les actes involontaires comme les erreurs et la possibilité d'actes intentionnels tels que la fraude. En fonction de leur secteur d’activité, chaque entreprise doit faire face à des menaces qui leur sont propres. Par exemple, une entreprise active dans le secteur de la navigation ne présente pas les mêmes risques qu’une entreprise active dans le secteur de la mode.

Pour repérer les risques, il est important de comprendre le processus interne de l’entreprise en identifiant les éléments qui créent le plus de valeur pour l’entreprise et ses vulnérabilités. Elle doit également identifier et évaluer les changements susceptibles d'avoir un impact significatif sur le système de contrôle interne.

À l’aide d’une cartographie des risques, l’organisation peut ensuite anticiper le risque en évaluant son impact et sa probabilité et prévoir les mesures nécessaires dans le but de limiter le risque en question.

Deux types de risque sont mis en avant. Le risque inhérent est la sensibilité d'un ensemble de comptes ou des transactions à des problèmes de contrôle importants en l'absence de contrôle interne. Le risque résiduel, quant à lui, est le risque qui subsiste après que la direction ait mis en place des contrôles internes ou d'autres réponses au risque.

Les entreprises doivent donc évaluer le risque inhérent, élaborer une réponse, puis évaluer le risque résiduel.

Pour aligner les risques identifiés sur la tolérance au risque de l'entreprise, la direction doit disposer d'une vue à l'échelle de l'entité. Ils doivent évaluer la probabilité et l'impact d'un risque, ainsi que les coûts et les avantages des réponses alternatives.

La direction peut répondre au risque de quatre manières :

- réduire la probabilité et l'impact du risque en mettant en place un système efficace de contrôle interne ;
- accepter la probabilité et l'impact du risque ;
- partager le risque ou le transférer en souscrivant une assurance, en externalisant une activité ;
- éviter le risque en ne s'engageant pas dans l'activité génératrice de risque. Cela peut se traduire par la vente d'un département, l'abandon d'une gamme de produits ou le fait de renoncer à se développer sur certains marchés.

Le service financier et le service d'audit interne aident la direction à concevoir des systèmes de contrôle efficaces pour réduire le risque inhérent. Ils évaluent également ces systèmes afin de s'assurer qu'ils fonctionnent efficacement.

À noter que les employés sont plus susceptibles de commettre une erreur que de commettre une fraude.

La probabilité et l'impact doivent être considérés comme un ensemble. Si ces deux éléments augmentent, le seuil de matérialité ainsi que la nécessité de se protéger contre cet événement augmentent également. Des logiciels aident à automatiser l'évaluation des risques ainsi que la réponse adéquate.

Ci-dessous une représentation schématique de la démarche :

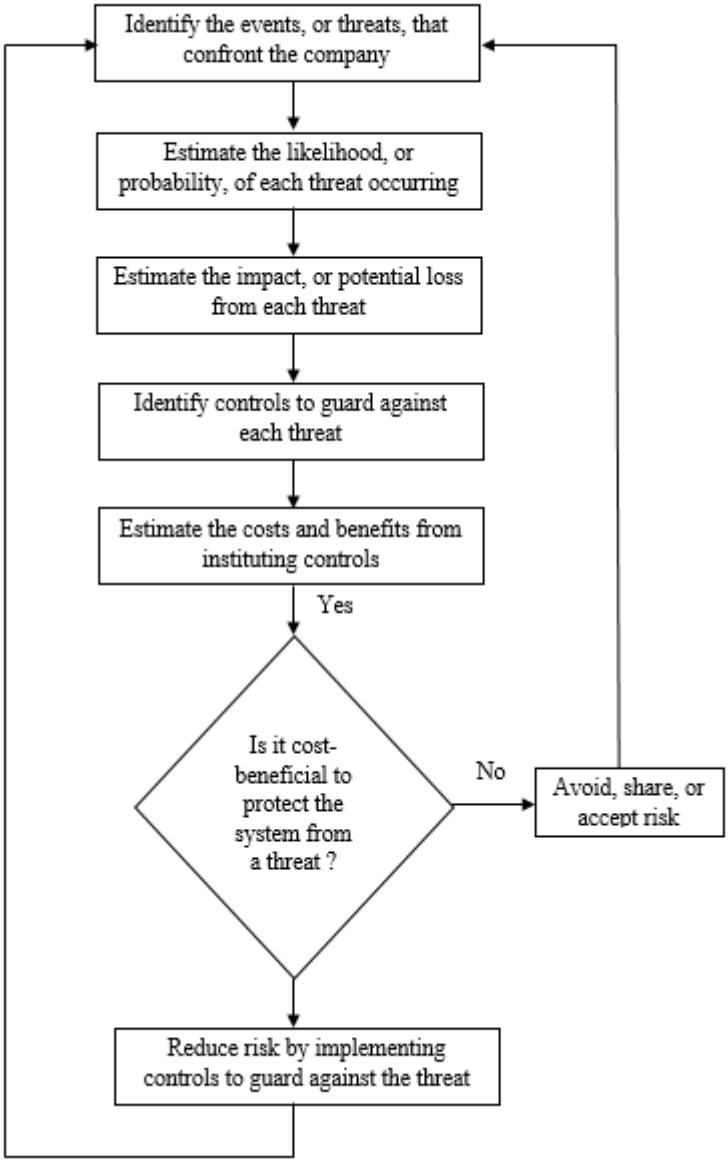



*Figure 8: Évaluation du risque et conception du contrôle interne (Romney & Steinbart 2016, 210)*

### 2.2.5. Activités de contrôle

Selon Romney et Steinbart (2016)[10], les activités de contrôle sont des politiques, des procédures et des règles qui fournissent une assurance raisonnable que les objectifs de contrôle sont atteints et les réponses aux risques sont mises en œuvre. Il revient à la direction de développer un système sûr et adéquatement contrôlé.

La direction doit s'assurer que :

- les contrôles sont sélectionnés et développés pour aider à réduire les risques à un niveau acceptable ;
- des contrôles généraux appropriés sont sélectionnés et développés sur la technologie en vigueur ;
- les activités de contrôle sont mises en œuvre et suivies comme spécifié dans les politiques et procédures.

Les contrôles sont beaucoup plus efficaces lorsqu'ils sont placés dans le système tel qu'il est construit, plutôt que comme une réflexion après coup. En conséquence, la direction doit impliquer les analystes de systèmes, les concepteurs et les utilisateurs lors de la conception de systèmes de contrôle informatisés.

Les procédures de contrôle entrent dans les catégories suivantes :

- autorisation appropriée des transactions et activités ;
- séparation des fonctions ;
- élaboration de procédures et contrôles d'acquisition ;
- contrôles de changement dans le management ;
- conception et utilisation des documents et des dossiers ;
- sauvegarde des actifs, des enregistrements et des données ;
- contrôles indépendants des performances.

[10] Romney, M. B. & Steinbart, P. J. (2016). *Accounting Information Systems* (14è éd.). New York: Pearson.

### 2.2.6. Information et communication

Les systèmes d'information et de communication doivent saisir et transmettre les informations nécessaires pour mener, gérer et contrôler les opérations de l'organisation.

Le but principal d'un système d'information comptable est de recueillir, d'enregistrer, de traiter, de stocker, de résumer et de communiquer des informations sur une organisation. Cela comprend la compréhension de la façon dont les transactions sont lancées, dont les données sont saisies, dont les fichiers sont consultés et mis à jour et comment les informations sont signalées. Cela inclut la compréhension des registres et des procédures comptables, des documents et des états financiers. Ces éléments fournissent une piste d'audit qui permet de retracer les transactions entre leur origine et les états financiers.

En plus d'identifier et d'enregistrer toutes les transactions valides, un système d'information comptable doit correctement classer les transactions, les enregistrer à leur valeur monétaire, enregistrer les transactions sur la période comptable appropriée et présenter correctement les transactions et les informations dans les états financiers.

La communication doit avoir lieu en interne et en externe pour fournir les informations nécessaires permettant de mener à bien les activités de contrôle interne quotidiennes.

Le cadre COSO IC mis à jour spécifie que les trois principes suivants s'appliquent au processus d'information et de communication:

- obtenir ou générer des informations pertinentes et de haute qualité pour soutenir le contrôle interne ;
- communiquer en interne les informations nécessaires, y compris les objectifs et les responsabilités, pour soutenir les autres composantes du contrôle interne ;
- communiquer les questions de contrôle interne pertinentes aux parties externes.

Les systèmes comptables se composent généralement de plusieurs sous-systèmes, chacun étant conçu pour traiter un type particulier de transaction utilisant les mêmes procédures. Il est donc question de comptabilité par cycles.

### 2.2.7. Surveillance

Le système de contrôle interne sélectionné ou développé doit être surveillé en permanence, évalué et modifié au besoin. Toute lacune doit être signalée à la direction et au conseil d'administration.

L'efficacité du contrôle interne est mesurée en utilisant une évaluation formelle ou une auto-évaluation. Une équipe peut être formée pour mener l'évaluation ou cela peut être fait par un audit interne.

Une supervision efficace implique la formation et l'assistance aux employés, la surveillance de leurs performances, la correction des erreurs et la supervision des employés qui ont accès aux actifs. La supervision est particulièrement importante dans les organisations sans définition claire des responsabilités ou séparation adéquate des fonctions. La séparation des fonctions au sein d'une entreprise est indispensable pour éviter de concentrer les risques entre les mains d'une même personne. Un exemple pour illustrer ce principe : une comptable du port autonome de Liège a été suspectée d'avoir détourné 30.000 EUR[11] lors d'un audit réalisé en 2019. Cette personne était à la fois comptable et trésorière de l'entreprise. Ce cas démontre clairement l'importance de mettre en place une séparation de fonctions entre la personne qui s'occupe de la comptabilité et celle qui encaisse l'argent.

Les activités du système de surveillance consistent à examiner des logiciels d'analyse et de gestion des risques, analyser les mesures de sécurité des ordinateurs et des réseaux, détecter les accès illégaux, tester les faiblesses et les vulnérabilités, signaler les faiblesses constatées et suggérer des améliorations.

Toutes les transactions et activités du système doivent être enregistrées dans un journal qui indique qui a accédé à quelles données, quand et à partir de quel appareil en ligne. Ce journal doit être examiné fréquemment pour surveiller l'activité du système, retracer les problèmes à partir de leur source, évaluer la productivité des employés, contrôler les coûts de l'entreprise, lutter contre l'espionnage et les attaques de piratage et se conformer aux exigences légales.

[11] RTBF info. (2019). *La Louvière : une comptable suspectée d'avoir détourné 30.000€ du port autonome*. En ligne https://www.rtbf.be/info/regions/detail_la-louviere-une-comptable-suspectee-d-avoir-detourne-30-000-du-port-autonome?id=10295012, consulté le 22 août 2019.

Des audits de sécurité externes, internes et de réseau peuvent évaluer et surveiller les risques ainsi que détecter les fraudes et les erreurs.

Informer les employés des audits aide à résoudre les problèmes de confidentialité, dissuade la fraude et réduit les erreurs. Les auditeurs doivent tester régulièrement les contrôles du système et parcourir périodiquement les fichiers d'utilisation du système à la recherche d'activités suspectes.

Les audits internes évaluent la fiabilité et l'intégrité des informations financières et opérationnelles, l'efficacité du contrôle interne et la conformité des employés aux politiques et procédures de gestion ainsi qu'aux lois et réglementations applicables.

Il est clair que le référentiel COSO ERM est un allié de poids en matière de gestion du risque, notamment dans le cadre de la problématique qui nous occupe. Cependant comme tout outil, il se heurte à de nombreuses limitations résultant de la qualité ou de la durabilité des objectifs établis dans le cadre d'un contrôle interne comme par exemple :

- le potentiel des jugements humains biaisés dans le cadre de la prise de décision ;
- la perception du management en matière de coûts/bénéfices en établissant des contrôles répondant aux risques ;
- la possibilité que les contrôles puissent être contournés en cas de collusion ;
- l'hypothèse du management override ;
- etc.

C'est pourquoi les différents contrôles mis en place ne peuvent fournir une assurance absolue quant à la réalisation des objectifs d'une entité. Notons néanmoins qu'un système de contrôle interne approprié joue un rôle important dans la prévention de la fraude.

# Chapitre 3. Mesures de prévention et de détection contre la fraude interne

Après avoir détaillé les types de fraude, leur déroulement et les facteurs qui y poussent, et décrit l'environnement de contrôle interne au sein d'une entreprise, ce chapitre aborde les différents moyens de prévention et/ou de détection à mettre en place pour permettre aux entreprises de faire face à une fraude éventuelle.

## 3.1. Structure de la gouvernance d'entreprise

Razali et Arshad (2014) ont démontré qu'une entreprise qui adopte une structure de gouvernance efficace réduit la probabilité d'émettre des rapports financiers frauduleux.

Suite à l'introduction du nouveau Code des sociétés et des associations, le Code belge de gouvernance d'entreprise a été mis à jour en 2020 et remplace désormais la version de 2009. Ce code s'applique aux sociétés de droit belge dont les actions sont négociées sur un marché réglementé.

La gouvernance d'entreprise peut être définie de la manière suivante :

> La gouvernance d'entreprise, encore appelée gouvernement d'entreprise, recouvre un ensemble de règles et de comportements qui déterminent comment les sociétés sont gérées et contrôlées. Une bonne gouvernance d'entreprise atteindra son objectif en établissant un équilibre adéquat entre le leadership, l'esprit d'entreprise et la performance, d'une part, et le contrôle ainsi que la conformité à ces règles, d'autre part. (Code belge de gouvernance d'entreprise 2009)

D'après l'étude menée par Razali et Arshad[12] (2014), trois composantes de la gouvernance d'entreprise permettent de réduire la probabilité de fraude dans les états financiers. Les résultats de cette étude ne permettent toutefois pas de tirer des conclusions générales. Cependant, les entreprises qui souhaitent se prémunir contre le risque de fraude peuvent mettre en place diverses mesures pour améliorer leur structure de gouvernance.

Tout d'abord, le Code des sociétés et associations prévoit que les sociétés cotées ont l'obligation de constituer un comité d'audit au sein de leur conseil d'administration. Afin de garantir la

[12] Razali, W.A.A.W.M., & Arshad, R. (2014). Disclosure of corporate governance structure and the likelihood of fraudulent financial reporting. *Procedia - Social and Behavioral Sciences*, *vol.145*, 243-253. doi: 10.1016/j.sbspro.2014.06.032.

qualité de l'information financière, le comité d'audit doit être constitué d'au moins trois membres. Il est composé de membres non exécutifs dont au moins un membre est un administrateur indépendant. Un administrateur non exécutif est une personne qui ne participe pas à la gestion journalière tandis qu'un administrateur indépendant doit répondre de plus au prescrit de l'article 7:87 qui renvoie à différents critères du Code de Gouvernance. La notion d'indépendance est très importante puisque le comité d'audit doit être en mesure de suivre l'élaboration de l'information financière ainsi que l'efficacité des systèmes de contrôle interne en toute impartialité.

Ensuite, l'audit interne a un rôle important dans la prévention contre la fraude. En effet, les auditeurs internes sont tenus d'évaluer l'efficacité du contrôle interne et sont donc plus à même de déceler les risques de fraude. De plus, pour assurer un fonctionnement efficace de l'audit interne, l'entreprise doit prévoir une interaction directe entre la fonction d'audit interne et le comité d'audit.

Enfin, le conseil d'administration doit être constitué d'une majorité d'administrateurs non exécutifs. De ce fait, ils ne subissent que rarement une pression de la part de l'organisation interne et peuvent agir de manière plus indépendante. De plus, leur position leur permet de dissuader les administrateurs exécutifs à commettre une fraude. Il est également conseillé que ces différents administrateurs aient des compétences et des expériences variées pour assurer une gestion efficace.

Pour assurer une meilleure gouvernance d'entreprise, les organisations peuvent s'inspirer des améliorations à mettre en place proposées par cette étude.

## 3.2. Code de conduite

Afin de garantir l'implication du personnel dans la lutte contre la fraude, l'entreprise doit prévoir un système de communication et de formation en interne. Les échanges d'informations peuvent s'exercer grâce aux newsletters, aux portails internet ou encore à des séminaires pour rappeler régulièrement l'importance de l'éthique professionnelle (Hassid & Masraff, 2010).

L'élaboration d'un code de conduite qui précise les comportements attendus et les pratiques interdites permet de faire comprendre aux membres du personnel la volonté de la direction à préserver l'intégrité de l'entité, notamment à travers une structure organisationnelle claire, une

politique concernant le conflit d'intérêts, l'existence d'un département d'audit interne. De plus, les employés prennent conscience des risques encourus en cas de fraude.

Cette mesure de prévention peut paraître assez élémentaire, mais certains fraudeurs essayent de justifier leurs actes en évoquant le fait qu'ils en ignoraient l'interdiction.

### 3.3. Système de lancement d'alerte

Les fraudes sont souvent décelées par hasard, mais l'entreprise peut mettre en place des moyens pour les détecter, notamment la création d'une ligne téléphonique permettant de lancer l'alerte (whistleblowing).

Les personnes témoins de comportements frauduleux sont souvent partagées par des sentiments contraires. Bien qu'elles souhaitent protéger les actifs de l'entreprise et signaler les fraudes, elles se sentent mal à l'aise à l'idée de lancer l'alerte et restent silencieuses. Cette réticence est d'autant plus forte si elles savent que leur carrière risque d'être compromise.

Une nouvelle directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 prévoit des dispositions visant à protéger les personnes qui signalent des violations du droit de l'Union européenne. Ces violations concernent plusieurs domaines tels que les marchés publics, le blanchiment de capitaux et le financement du terrorisme, la protection de l'environnement, la santé publique, la protection des consommateurs, etc. L'Europe interdit, à travers ces mesures de protection, toute forme de représailles comme la suspension, le licenciement, le changement de fonction, l'évaluation négative ou encore la discrimination. Les États membres doivent transposer cette directive dans leur droit national d'ici le 17 décembre 2021.

Cette disposition encourage donc de nombreuses entreprises à mettre en place un mécanisme de signalement permettant aux travailleurs d'avertir de façon anonyme tout soupçon de fraude.

### 3.4. Détection de signaux d'alerte

Wolfe et Hermanson (2004), les créateurs du diamant de la fraude, déclarent qu'il est nécessaire d'analyser le profil des travailleurs (compétences, emplois précédents, évaluations des performances, etc.) afin d'anticiper un éventuel cas de fraude. Pour ce faire, il peut être utile de discuter et de passer du temps avec la personne pour apprendre à la connaître. L'évaluation des

capacités de l'individu doit s'effectuer de manière continue car ce dernier peut adopter un autre comportement si, par exemple, du jour au lendemain, il occupe un poste à responsabilités. De plus, il peut être tenté de commettre une fraude lorsque les processus organisationnels ou les contrôles mis en place évoluent.

La direction peut également prévenir la fraude en détectant des signes avant-coureurs tel un changement de comportement ou de style de vie d'un employé (addiction à l'alcool, à la drogue ou au jeu, congés répétitifs, etc.). La direction peut alors mettre en place un système de soutien confidentiel pour aider ses employés à retrouver un certain équilibre (Petraşcu & Tieanu, 2014)[13].

### 3.5. Formations pour sensibiliser les cadres et les employés

De plus en plus de cabinets d'audit proposent diverses formations aux entreprises sur les risques de fraude. Ces experts forment les managers à prendre les bonnes décisions sur le plan éthique et informent l'entreprise des mécanismes de fraude existants pour lui permettre d'agir de manière préventive[14].

Un des membres du département *Forensic & Litigation Services* de BDO explique que ce sont majoritairement des entreprises de services publics qui font appel à leur service de formation. Ces formations sont assez généralistes et ne répondent pas forcément à une demande précise de l'entreprise. La formation vise à donner aux entreprises les bons réflexes d'analyse pour concevoir un contrôle interne efficace. Si l'équipe de formation devait orienter la formation en fonction de chaque entreprise, cela nécessiterait un travail beaucoup plus approfondi. En effet, il faudrait analyser l'environnement de la société, son secteur, son organisation interne (séparation des fonctions) et identifier ses faiblesses.

### 3.6. Mesures appropriées en cas de fraude

En cas de découverte d'une fraude, la direction doit agir de manière cohérente et appropriée, c'est-à-dire divulguer les informations à l'autorité compétente, fixer la hauteur du préjudice

[13] Petraşcu, D., & Tieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance*, *vol.16*, 489-497. doi: 10.1016/S2212-5671(14)00829-6.

[14] BDO. (2020). *Prévenir la fraude*. En ligne https://www.bdo.be/fr-be/services/audit-assurance/forensics-litigation-services/prevention-de-fraude, consulté le 5 avril 2020.

subi, identifier les causes et prendre les mesures nécessaires pour atténuer le risque de fraude et discuter avec les personnes concernées (Petraşcu & Tieanu, 2014).

Le personnel, quel que soit le poste occupé dans l'entreprise, doit être informé des conséquences et des sanctions encourues en cas d'implication dans une fraude. Les mesures prises par la direction doivent dissuader les potentiels fraudeurs et leur faire prendre conscience qu'une fraude est tôt ou tard détectée[15].

## 3.7. Outils d'analyse de données dans les entreprises

Avec l'apparition des nouveaux systèmes informatiques, la quantité des données à traiter a augmenté de manière exponentielle obligeant ainsi le personnel chargé du contrôle interne à utiliser des outils d'analyse de données. Ceux-ci peuvent être exploités par l'entreprise dans le cadre de la prévention et de la détection de la fraude.

L'analyse forensic de données (« Forensic Data Analytics ») se définit comme étant « la capacité de collecte et d'utilisation des données, à la fois structurées et non structurées afin de prévenir, détecter, surveiller ou investiguer des transactions potentiellement frauduleuses ou encore des faits ou comportements non éthiques » (EY - Étude mondiale 2018 sur l'analyse forensic de données).

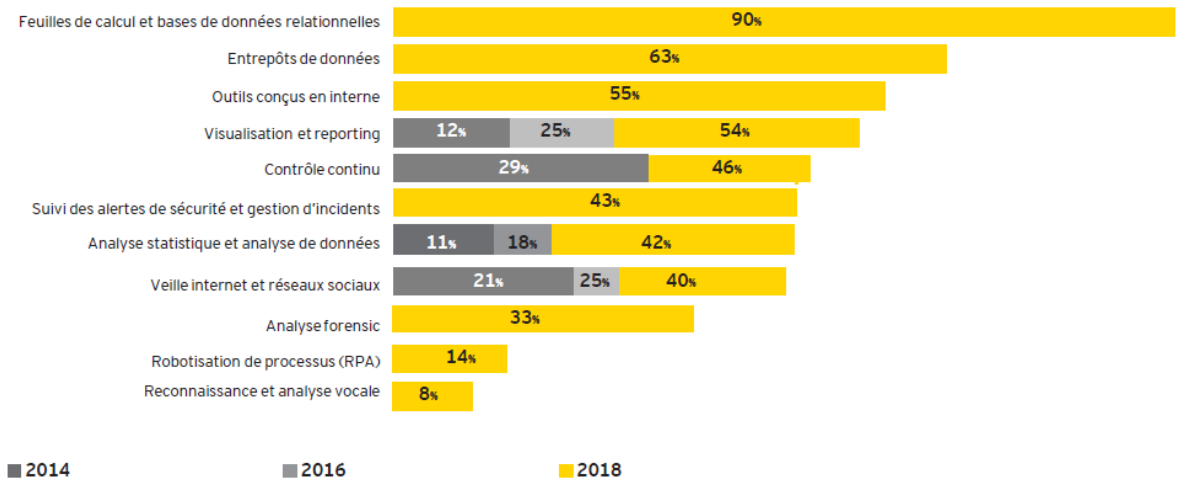



*Figure 9: Étude mondiale 2018 sur l'analyse forensic de données - EY*

[15] Petraşcu, D., & Tieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance, vol.16*, 489-497. doi: 10.1016/S2212-5671(14)00829-6.

En comparaison avec les années précédentes, les entreprises utilisent de plus en plus des technologies avancées pour gérer le risque de fraude (figure 9). Une étude mondiale sur l'analyse forensic de données (2018) reprend les différents outils utilisés par les entreprises. Ainsi, 90 % des participants déclarent utiliser des outils tels que Microsoft Excel. De plus, 46 % des répondants, contre 29 % en 2014, admettent avoir mis en place un système de contrôle continu au sein de l'entreprise. La surveillance d'informations sur internet et les réseaux sociaux est également utilisée dans 40 % des entreprises interrogées.

Selon Bănărescu[16], il existe deux types d'analyse de données : l'analyse opérationnelle et l'analyse stratégique.

L'analyse opérationnelle consiste à exploiter les données disponibles afin de détecter un éventuel cas de fraude. Ce type d'analyse remplace l'ensemble des activités manuelles et aide l'entreprise à identifier une fraude en examinant notamment les caractéristiques des suspects (position dans la hiérarchie du groupe, relation de subordination, etc.) ou encore le mode de communication (courrier électronique, réseaux sociaux). Afin de garantir le succès de cette approche, il est nécessaire d'utiliser différentes sources de données.

Quant à l'analyse stratégique, elle s'inscrit plutôt dans une approche macroéconomique en étudiant les menaces, les risques, les tendances d'évolution des phénomènes de fraude, l'évolution du marché ou le développement économique. À l'aide d'un grand volume de données, cette analyse porte tant sur les forces et les faiblesses de l'environnement interne que sur les opportunités et les menaces auxquelles une entreprise est confrontée dans son environnement extérieur.

Bien que l'intégration d'un outil d'analyse de données au sein d'un système de détection des fraudes soit avantageuse (réponses en temps réel, taux accru de détection des fraudes, réduction des erreurs, gain de temps, etc.), ces logiciels sont assez coûteux et n'intègrent pas nécessairement l'ensemble des données. De plus, certaines techniques permettent de détecter des cas de fraude sans justification claire et précise, facilitant ainsi le travail en sélectionnant les cas les plus suspects.

[16] Bănărescu, A. (2015). Detecting and preventing fraud with data analytics. *Procedia Economics and Finance*, *vol.32*, 1827-1836. doi: 10.1016/S2212-5671(15)01485-9.

## 3.8. Outils de détection de la fraude

Dans le cadre de l'audit, de nombreuses techniques de détection de la fraude financière existent pour extraire et découvrir les vérités cachées derrière de très grandes quantités de données. Bien que le sujet de ce mémoire ne traite pas spécifiquement du data mining, il est intéressant de mettre en évidence certains outils qui peuvent être utilisés par les auditeurs et réviseurs d'entreprises pour détecter des cas de fraude.

### 3.8.1. Analyse des ratios financiers

Les états financiers doivent représenter une image fidèle de la situation financière de l'entreprise. Pourtant, diverses manipulations comptables peuvent rendre ces états financiers frauduleux. Suivant l'élément de pression repris dans le triangle de la fraude, nul doute qu'une entreprise confrontée à des difficultés financières ou qui souhaite améliorer ses résultats peut être tentée de manipuler ses états financiers. C'est pourquoi Kanapickienė et Grundienė (2015) considèrent que l'analyse des ratios financiers est une méthode pertinente pour identifier les fraudes. La technique qu'ils proposent consiste à identifier les ratios financiers qui présentent une différence statistiquement significative entre les états financiers frauduleux et non frauduleux et à fournir un modèle de régression logistique utile pour détecter des états financiers frauduleux.

Le tableau ci-dessous reprend les principaux ratios à analyser en fonction de la situation financière de l'entreprise et indique les rubriques qui sont souvent sujettes à des manipulations.

| | | **Ratios à analyser** |
|---|---|---|
| **Situation de l'entreprise** | Difficultés financières (niveau d'endettement élevé, manque de liquidité) | - Total des dettes sur le total actif<br>- Total des dettes sur les fonds propres<br>- Total passif sur le total actif<br>- Fonds de roulement sur le total actif<br>- Actifs circulants sur les dettes à court terme |
| | Volonté de croissance | - Total des ventes sur l'actif total<br>- Bénéfice net sur le total des ventes<br>- Bénéfice net sur l'actif total<br>- Actifs circulants sur le total actif |

| | | |
|---|---|---|
| **Rubriques à contrôler** | Manipulation de la marge brute | - Marge brute sur le total des ventes<br>- Marge brute sur le total des actifs |
| | Manipulation des stocks et des créances clients | - Stocks sur le total des ventes<br>- Stocks sur le total de l'actif<br>- Créances clients sur le total des ventes |

*Tableau 1: Analyse des ratios dans les états financiers (Kanapickienė & Grundienė 2015, 322)*

Grâce à la méthode de régression linéaire multiple, quatre auteurs[17] ont identifié que deux ratios financiers, à savoir les créances sur les recettes et le levier financier, donnent un résultat significatif pour prédire les rapports financiers frauduleux. En effet, les entreprises frauduleuses ont tendance à surévaluer le montant de leurs créances. De plus, le levier financier se mesure par le rapport entre la dette totale et les capitaux propres. Plus l'effet de levier est important, moins l'entreprise a de chance d'obtenir un prêt supplémentaire. Dans ce cas, la probabilité de fraude est donc plus élevée.

Ces résultats doivent être interprétés avec prudence car chaque cas de fraude est différent. Certains ratios financiers qui ne sont pas pertinents pour une entreprise peuvent l'être pour une autre.

L'identification des ratios financiers semble facile à appréhender. Cependant, il est difficile de savoir si les valeurs des ratios financiers permettent d'indiquer des états financiers frauduleux ou non.

La recherche menée par Kanapickienė et Grundienė (2015) a été effectuée en utilisant des états financiers frauduleux (groupe expérimental) et non frauduleux (groupe de contrôle). Dans la première phase de recherche, l'objectif est de tester une cinquantaine de ratios utiles pour détecter la fraude. Chaque ratio financier est alors examiné dans les états financiers frauduleux et non frauduleux.

Ensuite, les ratios financiers qui proviennent d'une population normalement distribuée sont étudiés à l'aide du t-test. Dans ce cas, l'hypothèse d'égalité des moyennes est vérifiée.

[17] Dalnial, H., Kamaluddin, A., Sanusi, Z.M., & Khairuddin, K.S. (2014). Accountability in financial reporting: detecting fraudulent firms. *Procedia - Social and Behavioral Sciences, vol.145*, 61-69. doi: 10.1016/j.sbspro.2014.06.011.

L'hypothèse nulle (H0) selon laquelle les moyennes des ratios financiers ne diffèrent pas dans les états financiers frauduleux et non frauduleux est rejetée si la p-valeur est inférieure à α (α= 0,05). Si l'hypothèse de normalité n'est pas valide, les ratios sont étudiés à l'aide du test U de Mann Whitney.

Sur l'ensemble des ratios sensibles à la fraude, les résultats de la recherche permettent de sélectionner ceux qui pourraient indiquer un risque de fraude.

Sur base de ces tests statistiques, il a été déterminé qu'il existe un problème de multicolinéarité dans ces modèles. En effet, certains ratios sont calculés à partir des mêmes valeurs et sont donc des combinaisons des uns des autres. Par conséquent, ces modèles doivent être améliorés grâce à la sélection d'un sous-ensemble de ratios permettant de déterminer un maximum d'informations, sans redondance. Sur base des ratios sélectionnés, Kanapickienė et Grundienė (2015) ont développé un modèle de régression logistique où la probabilité de fraude est calculée comme suit :

$$P = 1 / (1 + e^{5,768 - 4,263 \times S/TA - 0,029 \times V/AI - 4,766 \times D/TA - 1,936 \times VD/DCT})$$

P est la probabilité de fraude dans les états financiers (de 0 à 1) ; S/TA – Stocks/Total actif ; V/AI – Ventes/Actifs immobilisés ; D/TA – Dettes/Total actif ; VD/DCT – Valeurs disponibles/Dettes à court terme.

Il peut être intéressant d'appliquer ce modèle à un cas réel à titre purement illustratif. Par exemple, les comptes 2018[18] de Pairi Daiza, un célèbre parc animalier situé à Cambron-Casteau en Belgique. Les valeurs reprises dans le tableau ci-dessous sont issues de la Banque Nationale de Belgique.

| **Comptes** | **Valeurs (EUR)** |
|---|---|
| Stocks | 1.770.034 |
| Total de l'actif | 166.279.710 |
| Ventes et prestations | 71.285.635 |
| Total des dettes | 133.791.854 |
| Actifs immobilisés | 136.111.307 |
| Valeurs disponibles | 18.410.092 |
| Dettes à un an au plus | 29.803.167 |

*Tableau 2: Comptes 2018 Pairi Daiza*

[18] Banque Nationale de Belgique. (2019). *Comptes annuels 2019 Pairi Daiza*. En ligne https://cri.nbb.be/bc9/web/catalog;jsessionid=578FD3CA7ACFBB3BFB133905077AA4DC?execution=e1s3, consulté le 17 avril 2020.

Après avoir calculé les différents ratios, les valeurs obtenues dans le modèle de base sont intégrées. La probabilité obtenue étant inférieure à 50 %, le risque que les états financiers soient frauduleux est faible.

$$P = 1 / (1 + e^{5,768 - 4,263 \times 0,01 - 0,029 \times 0,52 - 4,766 \times 0,80 - 1,936 \times 0,62}) = 0,33$$

Ce modèle peut être employé comme indicateur par des utilisateurs externes pour identifier des états financiers frauduleux. Cependant, il est nécessaire de rappeler qu'il revient à l'auditeur d'évaluer le risque de fraude et d'effectuer des tests complémentaires si nécessaire.

### 3.8.2. Séparateurs à vaste marge (SVM)

Grâce à la création d'un espace de plus grande dimension, la méthode des séparateurs à vaste marge (SVM)[19] permet de déterminer une fonction linéaire pour séparer les données en plusieurs classes, à savoir les cas frauduleux et non frauduleux. La figure 10 illustre la marge maximale, c'est-à-dire la distance entre la frontière de séparation et les vecteurs de support.

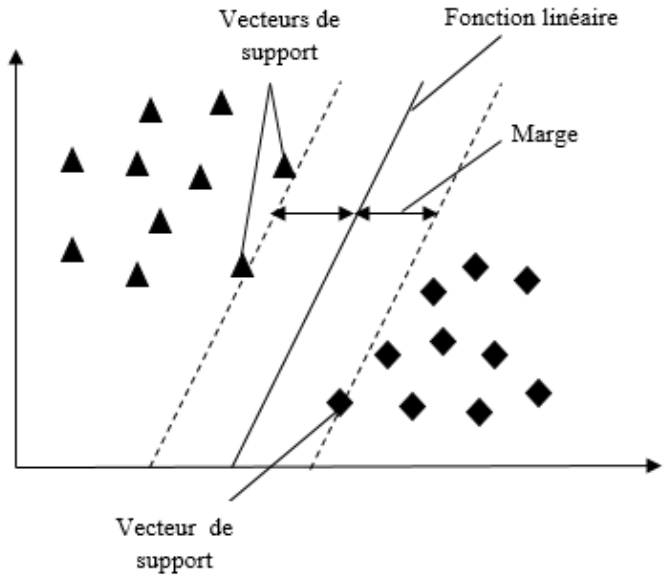



*Figure 10: Illustration de la méthode SVM*

[19] West, J., Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. *Computers & Security*, *vol.57*, 47-66. doi: 10.1016/j.cose.2015.09.005.

Thomas Meurice, directeur chez PricewaterhouseCoopers (PwC), explique concrètement l'application de cet outil dans le domaine de l'audit.

Il apparaît que la plupart des auditeurs externes et réviseurs d'entreprises utilisent le modèle SVM sans vraiment connaître son fonctionnement interne. Tout d'abord, le modèle est entraîné grâce à un jeu de données test afin que le système comprenne les transactions constituant un risque de fraude élevé et les transactions normales. Ensuite, les professionnels du chiffre vont collecter toutes les données comptables de l'entreprise auditée et les insérer dans le système. Celui-ci évalue alors ces transactions et repère celles dont le risque de fraude est élevé. Les transactions considérées comme frauduleuses sont analysées en détail par le professionnel qui juge si des tests complémentaires doivent être effectués.

Un lien peut être fait avec la méthode précédente. En effet, au lieu d'utiliser des transactions comptables, il est possible d'utiliser des ratios financiers. Les ratios financiers peuvent être sélectionnés à l'aide des tests d'hypothèse expliqués dans l'article de Kanapickienė et Grundienė (2015)[20]. Le jeu de données d'entraînement du modèle devient donc une base de données regroupant les différents ratios avec le bon libellé (frauduleux vs non frauduleux). Dans le cas d'une analyse, l'auditeur n'a qu'à encoder les valeurs des ratios précédemment sélectionnés pour que le système évalue le risque de fraude.

### 3.8.3. Arbres de décision

Une structure arborescente, appelée arbre de décision, illustre un ensemble de règles en cascade. Chaque nœud représente alors un test et chaque branche représente un résultat du test (Sadgali, Sael, & Benabbou, 2019).

Sur base des propos recueillis par un réviseur d'entreprises de BDO et membre du département *Forensic & Litigation*[21], les professionnels du chiffre peuvent utiliser l'arbre de décision pour analyser l'ensemble des achats d'une entreprise et sélectionner les factures suspectes. Pour chaque facture, il y a d'abord lieu d'examiner les transactions qui ont été approuvées et encodées par la même personne. Ensuite, parmi les factures dont la séparation des fonctions n'est pas respectée, l'étape suivante consiste à sélectionner les achats supérieurs à 1.000 EUR.

[20] Kanapickienė, R., & Grundienė, Ž. (2015). The model of fraud detection in financial statements by means of financial ratios. *Procedia - Social and Behavioral Sciences, vol.213,* 321-327. doi: 10.1016/j.sbspro.2015.11.545.

[21] Cfr annexe 6 : Interview de Jean-François Bernard page A41

En effet, certains professionnels estiment que commettre une fraude pour un montant inférieur à 1.000 EUR est peu probable. La figure ci-dessous illustre les différents tests effectués et les résultats obtenus sous forme d'une structure arborescente.

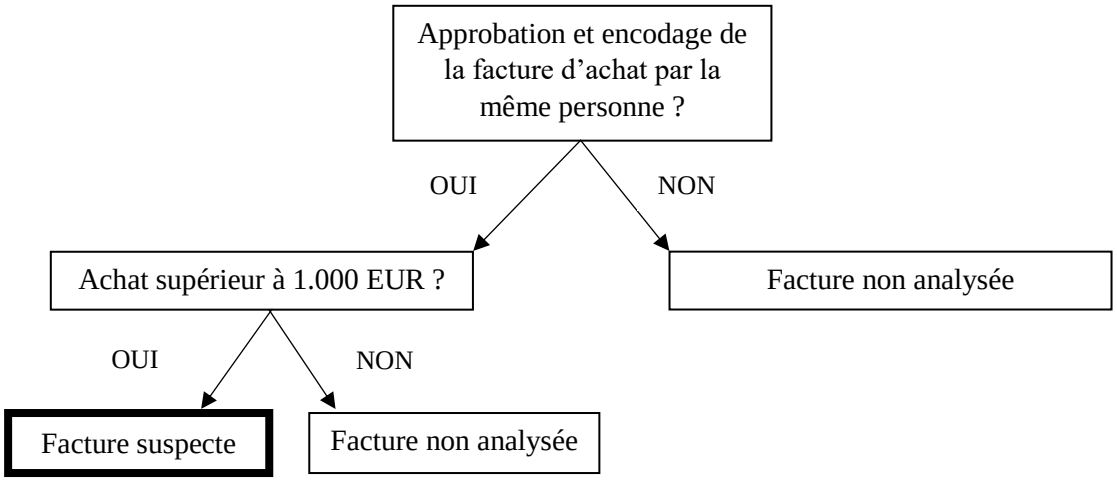



*Figure 11: Arbre de décision (exemple 1)*

Ce réviseur d'entreprises a également expliqué un cas de surfacturation pour un chantier de travaux publics. Le fournisseur devait placer des chambres de visite d'un mètre cube. La fourniture de services prévoit la quantité de terre mise en décharge et la quantité de remblai. Normalement, la société de services était supposée facturer un mètre cube de terre à mettre en décharge et un mètre cube de remblai. L'analyse consistait alors à sélectionner tous les chantiers du fournisseur qui impliquaient le placement du même modèle de chambre de visite et à filtrer ceux pour lesquels la quantité de terre à évacuer et de remblai facturée était supérieure à trois fois la quantité attendue. Le raisonnement est schématisé à l'aide de la figure suivante.

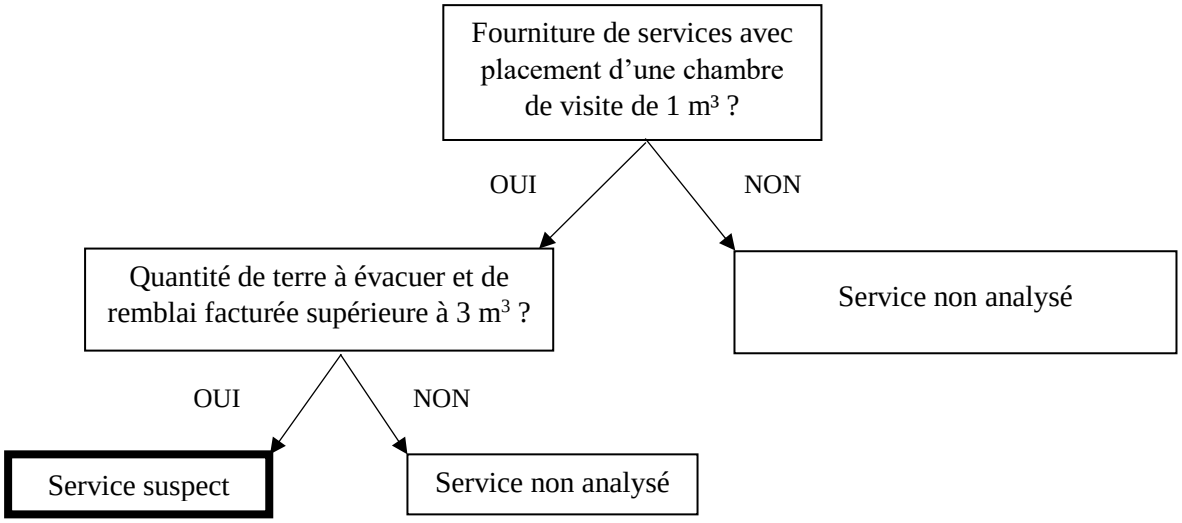



*Figure 12: Arbre de décision (exemple 2)*

Cette méthode dont le but est donc de poser toute une série de questions pour se concentrer sur l'analyse d'un nombre limité de transactions présente l'avantage non négligeable d'être facilement interprétable. Ces arbres de décision permettent d'identifier les facteurs importants afin de détecter une fraude.

### 3.8.4. Text mining

Le text mining consiste à extraire des données à partir de textes[22]. Afin de transformer le texte brut en données quantitatives, celui-ci subit divers traitements comme par exemple le filtrage des mots, la suppression du pluriel et des temps, l'analyse de fréquence des mots, etc. L'exploration des données permet ensuite d'effectuer une classification entre toutes les informations recueillies.

Toujours sur base de l'interview réalisée avec le réviseur d'entreprises de BDO[23], le text mining est utilisé pour détecter des cas de fraude. À titre d'exemple, son équipe suspectait un cas de fraude relatif à des services de conseil entre un fournisseur et le secrétaire général d'une association, facturés à 500.000 EUR. En effet, aucun contrat hormis des factures dont les libellés étaient assez lacunaires ne pouvait démontrer le service fourni. De ce fait, les réviseurs d'entreprises ont tenté de prouver qu'aucun service n'a été rendu. Ils ont considéré que des

[22] West, J., Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. *Computers & Security, vol.57,* 47-66. doi: 10.1016/j.cose.2015.09.005.

[23] Cfr annexe 6 : Interview de Jean-François Bernard, page A41

services de conseil s'élevant à 500.000 EUR nécessitaient automatiquement des échanges de mails entre la personne qui commande le service et celui qui le preste. Ils ont alors analysé la boîte mail du client en recherchant des mots-clés (nom de la société fournisseur, prénom et nom de l'actionnaire) parmi les mails reçus et envoyés. Sur une période de deux ans, un seul mail a été échangé entre les deux parties. Grâce à la technique du text mining, les professionnels ont réussi à démontrer que la relation était fictive.

Cet outil d'analyse de données est particulièrement utile dans le cadre de la fraude aux états financiers étant donné qu'une grande quantité de données textuelles est disponible.

### 3.8.5. Loi de Benford

À la fin des années 30, la loi Benford voit le jour. Cette loi statistique permet de mettre en évidence la fréquence d'apparition du premier chiffre d'un nombre dans une série de nombres (Bonache, Maurice & Moris, 2010). La probabilité pour que la valeur *d* apparaisse en première position est calculée grâce à la formule empirique : log (1+1/*d*). La valeur *d* représente le chiffre significatif, c'est-à-dire le chiffre le plus à gauche différent de 0.

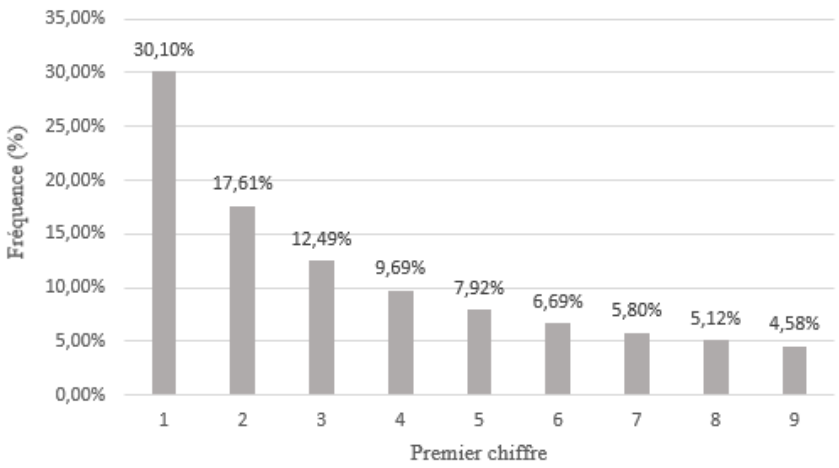



*Figure 13: Loi de Benford*

Le graphique ci-dessus montre que la fréquence d'apparition du chiffre 1 en première position dans une série de nombres est de 30,10 %.

À la fin des années 1980, cette loi statistique est utilisée dans la détection des fraudes comptables en comparant la loi de Benford avec la distribution des chiffres comptables d'une

entreprise. Lorsqu'une différence significative entre les deux distributions apparaît, il est possible que l'auditeur soit en présence d'une fraude. Il y a donc lieu de mener des recherches plus approfondies pour collecter des éléments probants.

Il est utile de préciser que certaines fraudes ne peuvent pas être décelées par la loi de Benford, comme par exemple les transactions qui ne font pas l'objet d'un enregistrement comptable (vols, pots-de-vin, etc.) ou les séries de données fixées de manière arbitraire (numéros de factures). Dans ce cas, les auditeurs devront mettre en œuvre des méthodes non statistiques à savoir l'évaluation du contrôle interne de l'entreprise et l'analyse des documents comptables.

De plus, les secteurs de produits innovants et/ou à la mode peuvent ne pas être en adéquation avec la loi de Benford (Bonache et al., 2010).

L'auditeur externe devra dans tous les cas faire preuve d'esprit critique par rapport à cette technique de détection des fraudes.

## 3.9. Forensic accounting

Afin de détecter la fraude, une solution à envisager peut être le recours à des spécialistes dédiés.

En Amérique du Nord, un groupement professionnel de près de 30 000 membres spécifiquement formés à la problématique a vu le jour en 1988 à l'initiative de l'Association of Certified Fraud Examiners (ACFE).

À l'heure actuelle, il n'existe pas de telle organisation en Europe.

Ces professionnels disposent d'une grande expérience en matière de fraude et de pratiques illicites, mais aussi en matière de techniques d'investigation.

Le terme « forensic accounting » désigne l'intégration de compétences comptables, d'audit et d'investigation. Il s'agit de l'application de concepts et de techniques comptables aux problématiques de fraude[24].

Ces spécialistes établissent des rapports pouvant servir de preuve auprès d'un tribunal ou dans des procédures administratives.

[24] Accouting.com. (2020). *What is forensic accounting ?* En ligne https://www.accounting.com/resources/forensic-accounting-basics/, consulté le 9 février 2020.

Un audit en forensic accounting nécessite un cheminement différent d'un audit d'états financiers. Chaque situation requiert un protocole unique.

Ce processus implique une investigation, un reporting et finalement, la conduite du litige final.

Ces spécialistes entament généralement une enquête et recueillent des éléments de preuve lorsque des soupçons de fraude existent déjà. Dans cette phase d'enquête, ils sont à la recherche de signaux d'alerte et d'écarts pouvant indiquer qu'une fraude a eu lieu. En utilisant les informations recueillies, ils formulent une hypothèse sur ce qui s'est passé et élabore des procédures de suivi afin de continuer à évaluer l'organisation.

Une fois la phase de récolte des informations achevée, le forensic accountant établit un rapport où il présente un résumé de ses conclusions au personnel compétent. Ensuite, le spécialiste détermine la marche à suivre pour traiter le dossier.

Ils peuvent également formuler des recommandations en termes de moyens de prévention de fraude à l'avenir.

La dernière étape du processus implique la participation de ce spécialiste en tant qu'expert dans une éventuelle procédure judiciaire. Il est donc amené à présenter les éléments de preuve, mais aussi à interpréter les documents financiers. Cela signifie qu'il doit non seulement trouver des preuves, mais il doit aussi être en mesure d'utiliser une rhétorique ayant du sens pour un tribunal.

# Chapitre 4. Rôle de l'auditeur externe dans le processus

Zager, Sever Malis, et Novak (2016) estiment que la direction, le conseil d'administration, le comité d'audit, les auditeurs internes ainsi que les auditeurs externes ont tous un rôle important dans l'entreprise et doivent tout mettre en œuvre pour garantir la fiabilité des états financiers. Après avoir passé en revue les responsabilités de ces différents organes, ce chapitre traite le rôle spécifique de l'auditeur externe dans le cadre de la prévention et la détection de la fraude.

## 4.1. Responsabilités des principaux acteurs de l'entreprise

Conformément à la norme ISA 240, la responsabilité première en matière de fraude incombe à la fois à la direction et aux responsables de la gouvernance de l'entreprise. Il est important que la direction, sous la supervision des responsables de la gouvernance, travaille à prévenir la fraude en éliminant les opportunités d'occurrence de celle-ci et en créant une culture d'éthique et d'honnêteté forte à l'échelle de l'entité.

Bien que la direction soit responsable de l'élaboration d'un système de contrôle interne efficace, le risque qu'elle contourne les contrôles mis en place, manipule la comptabilité ou présente une information financière mensongère est assez élevé. Il est donc essentiel de définir les rôles et les responsabilités des autres parties prenantes de l'entreprise dans la prévention et la détection de la fraude.

Le conseil d'administration contrôle les actions de la direction tandis que le comité d'audit examine le programme de travail de l'auditeur interne tout en tenant compte de la complémentarité entre la fonction de l'audit interne et celle de l'audit externe.

Les normes d'audit interne définies par l'IIA (The Institute of Internal Auditors) démontrent l'importance de l'audit interne en matière de fraude. En effet, « les auditeurs internes doivent posséder des connaissances suffisantes pour évaluer le risque de fraude et la façon dont ce risque est géré par l'organisation » (IIA, 2017). Les auditeurs internes doivent notamment maîtriser les différents scénarios de fraude possibles directement en lien avec l'activité de l'entreprise pour laquelle ils travaillent (Petraşcua & Tieanu, 2014).

## 4.2. Responsabilités de l’auditeur externe

La norme internationale d’audit ISA 240 traitant des responsabilités de l’auditeur externe en matière de fraude dans un audit des états financiers est probablement l’une des normes mise en évidence et largement révisée après les nombreux scandales dans le monde des affaires.

La responsabilité de l’auditeur externe consiste à exprimer une opinion sur les états financiers pour lesquels il est tenu d’obtenir une assurance raisonnable. Afin d’exprimer une opinion sur l’image fidèle des états financiers, il doit être certain que ces derniers sont exempts d’inexactitudes importantes dues à la fraude ou à l’erreur. Pour obtenir une assurance raisonnable, l'auditeur doit faire preuve d'esprit critique tout au long de l'audit et prendre en compte la possibilité que les dirigeants contournent les contrôles en place. De plus, l’auditeur externe doit être conscient du fait que des procédures d'audit qui sont efficientes pour détecter des erreurs peuvent ne pas l'être pour la détection de fraudes.

L'auditeur a également un rôle de prévention vis-à-vis de l’entité auditée, car il doit communiquer de façon appropriée aux personnes constituant le gouvernement d'entreprise et à la direction les faiblesses du contrôle interne qu'il a relevées au cours de l'audit et qui, selon son jugement professionnel, sont suffisamment importantes pour mériter leur attention.

Il est important de signaler que l’auditeur a une obligation de moyen et non pas une obligation de résultat. En effet, le risque de ne pas détecter une anomalie significative provenant de fraudes est élevé étant donné que la fraude peut résulter de procédés sophistiqués et qu’il existe des limitations inhérentes à un audit (difficulté d’assurer l’exhaustivité, disponibilité des éléments probants, etc.) même si l’audit est correctement planifié et exécuté. Cela devient encore plus difficile si la fraude en question implique la direction (par opposition à une fraude commise par un employé) car cette dernière est tout à fait capable de contourner les activités de contrôle, de concevoir et de modifier les politiques et processus mis en place.

C’est pourquoi si des anomalies significatives sont identifiées par l’auditeur à la suite de procédures d’audit, ce dernier doit examiner si elles résultent d’une fraude ou d’une erreur et doit concevoir d’autres procédures d’audit afin d’obtenir des éléments probants suffisants et appropriés par rapport au risque évalué et enfin concevoir des réponses adéquates.

### 4.2.1. Caractéristiques de la fraude

Dans la vie économique, la fraude peut survenir pour un certain nombre de raisons et prendre différentes formes, mais l'auditeur est intéressé spécifiquement par des activités frauduleuses susceptibles de provoquer des anomalies significatives dans les états financiers. Il s'intéresse donc à deux types d'anomalies intentionnelles :

- les anomalies résultant de l'élaboration d'informations financières mensongères ;
- les anomalies résultant d'un détournement d'actifs.

Notons que les anomalies peuvent être causées soit par la fraude, soit par l'erreur. Le facteur déterminant l'appartenance à une catégorie plutôt qu'à une autre est l'aspect intentionnel ou non de l'acte posé. Si l'acte n'est pas intentionnel, les effets observés ne seront probablement pas si profonds et peuvent être considérés comme un événement ponctuel causé par une erreur humaine ou une négligence.

Par contre, si le caractère intentionnel est présent, l'instigateur de la fraude essaiera de camoufler son acte afin qu'il ne soit pas découvert. Ce processus d'habillage des comptes va très probablement affecter l'information financière à de nombreux niveaux et entraînera des anomalies significatives.

### 4.2.2. Évaluation du risque de fraude

Bien qu'il puisse atténuer les risques inhérents, il existe toujours une probabilité que le système de contrôle interne n'ait pas empêché une erreur significative. Outre les limitations du contrôle interne, certaines circonstances sont susceptibles d'augmenter le risque de fraude. Il s'agit notamment des aspects liés à l'intégrité de la direction, des transactions inhabituelles ou encore la difficulté d'obtenir des éléments probants suffisants et appropriés. De plus, l'auditeur doit évaluer le risque de fraude en se fondant sur la présomption qu'il existe un risque dans la comptabilisation des produits.

Dans le cadre de l'évaluation des risques, l'auditeur va avoir recours à trois mécanismes : son scepticisme professionnel, discuter avec les membres de l'équipe d'audit et mettre en œuvre des procédures d'évaluation du risque.

#### *4.2.2.1. Scepticisme professionnel*

La norme ISA 200 a exigé de l'auditeur qu'il effectue l'audit avec une attitude de scepticisme professionnel, ce qui implique de rester vigilant vis-à-vis des indicateurs et des possibilités qui peuvent potentiellement entraîner une fraude. Être sceptique ne signifie pas que l'auditeur doit évaluer l'exactitude de chaque dossier transmis par la direction. L'auditeur ne soupçonnera une fraude que s'il y a des raisons valables, auquel cas il approfondira ses recherches. Son expérience en matière d'honnêteté de la direction ne doit pas réduire l'approche sceptique et le pousser à ignorer les raisons pour lesquelles les informations financières sont inexactes et les généraliser comme des erreurs. Si une incohérence est constatée, l'auditeur doit enquêter sur la question.

#### *4.2.2.2. Discussion au sein de l'équipe d'audit*

Afin que les missions d'audit soient efficaces, une discussion au sein des membres de l'équipe est primordiale ainsi qu'une communication proactive avec le personnel impliqué dans la gestion de l'entité. Dans l'éventualité où une fraude serait suspectée ou identifiée, l'auditeur doit déterminer ses effets sur la mission d'audit ainsi que documenter son travail et les mesures ayant été prises pour traiter les problèmes rencontrés.

Ces discussions peuvent porter sur les rubriques des états financiers susceptibles de comporter des anomalies significatives, la façon dont les actifs de l'entreprise pourraient être détournés ou encore les facteurs internes et externes pouvant inciter des individus à commettre une fraude.

#### *4.2.2.3. Procédure d'évaluation du risque de fraude*

La norme ISA 240 prévoit certaines lignes directrices concernant l'évaluation du risque de fraude. En matière de procédures d'évaluation des risques, l'axe principal est la demande d'informations. En sollicitant la direction, les employés et les auditeurs internes, l'auditeur externe peut identifier les conditions et les événements indiquant une fraude. Ce mécanisme aide également à évaluer si la direction et les responsables de la gouvernance remplissent leurs fonctions en matière de prévention et de détection de la fraude.

L’auditeur se renseigne auprès de la direction notamment sur:

- l’évaluation de la fraude ;
- les systèmes de gestion mis en place pour prévenir, détecter et répondre aux fraudes identifiées ou suspectées;
- la communication entre la direction et les responsables de la gouvernance concernant le système en place pour évaluer et répondre au risque de fraude;
- les instructions de la direction aux employés, comme par exemple les bonnes pratiques ou le code de conduite.

L’auditeur doit également demander à la direction, aux personnes concernées ou aux responsables de la fonction d’audit interne si elles ont connaissance d’une fraude suspectée ou identifiée ou s’il existe des éléments indiquant une fraude potentielle.

À moins que les responsables de la gouvernance ne fassent partie de la direction, l’auditeur doit les interroger quant à la supervision de la gestion, du système de contrôle interne. Cela permet d’aider l’auditeur à corroborer les demandes de renseignements auprès de la direction.

Selon certains auteurs cités par Petraşcua et Tieanu (2014), l’auditeur doit, lors de l'évaluation du risque de fraude, se poser plusieurs questions. Celles-ci portent par exemple sur le mode de rémunération de la direction et des employés, la rigueur des contrôles internes, la motivation du personnel à commettre une fraude ou des changements majeurs au sein de l'organisation.

Il est utile de préciser que l’évaluation des risques liés au contrôle est basée sur les composantes du référentiel COSO reprises dans le chapitre 2.

Le processus d’évaluation du risque de fraude comporte les étapes suivantes :

1. organiser la manière d'évaluer les risques de fraude (stratégie globale d’audit) ;
2. identifier les différents scénarios de fraude possibles ;
3. évaluer les possibilités de commettre des fraudes ;
4. évaluer le degré d'importance des risques de fraude identifiés ;
5. prendre connaissance du contrôle interne existant et identifier ses faiblesses ;

6. élaborer ou modifier le plan d'audit sur base des résultats de l'évaluation des risques de fraude.

Les procédures analytiques sont un outil non négligeable en matière d'identification d'informations non conformes aux attentes. L'auditeur peut utiliser ces procédures dans le cadre de l'évaluation du risque de fraude. Si de telles incohérences sont constatées, il devra évaluer les éléments mis à sa disposition. L'auditeur analyse aussi toute autre information s'ajoutant au système de reporting de l'entité afin d'enquêter sur d'éventuelles données incompatibles avec celles qu'il détient déjà.

Lors de l'exécution des procédures d'évaluation des risques, l'auditeur obtient souvent des informations concernant l'existence de facteurs de risque de fraude. Dans la norme ISA 240, ceux-ci se définissent comme étant des « faits ou conditions porteurs d'une incitation ou d'une pression à commettre une fraude ou qui fournissent une opportunité de la commettre ». Ils ont été abordés précédemment dans le cadre de l'analyse du triangle de la fraude. Bien que l'existence de tels facteurs ne signifie pas automatiquement que la fraude existe, des anomalies significatives peuvent apparaître dans les états financiers.

Une étude réalisée en Malaisie[25] a démontré qu'il existe une relation significative entre les facteurs de risque de fraude, à savoir le système de contrôle interne (opportunité), la pression et le type d'auditeurs (internes et externes), et le jugement de l'auditeur en matière d'évaluation du risque de fraude. Tout d'abord, il est évident que l'efficacité du système de contrôle interne est liée à la probabilité du risque de fraude. Si le contrôle interne présente des faiblesses significatives, les programmes d'audit doivent être adaptés en élargissant les tests de détail. Ensuite, la pression ou le besoin est l'un des facteurs qui incite fortement les auteurs à se comporter de manière illégale. Les auditeurs doivent tenir compte de ce facteur lors de la phase de l'évaluation des risques. Enfin, les auditeurs internes et externes ont une capacité similaire à porter un jugement sur l'évaluation des risques de fraude.

Cette étude permet donc de conclure que l'efficacité d'un audit dépend de la capacité de l'auditeur à évaluer les risques avec précision. La non-détection d'une inexactitude significative dans les états financiers peut entraîner une insatisfaction auprès des tiers et porter atteinte à la réputation de l'auditeur.

[25] Mohd-Sanusi, Z., Khalid, N.H., & Mahir, A. (2015). An evaluation of clients' fraud reasoning motives in assessing fraud risks: from the perspective of external and internal auditors.

### 4.2.3. Réponse au risque évalué : évaluation des éléments obtenus

L'auditeur doit mettre en œuvre des procédures d'audit en réponse aux risques évalués d'anomalies significatives provenant de fraudes.

Une approche générale consisterait à remanier les procédures de telle sorte qu'elles laissent moins de marche de manœuvre en termes de fraude. Il s'agit aussi de superviser et assigner les tâches aux membres de l'équipe en fonction de leurs connaissances, compétences et expérience suivant le risque de fraude évalué. Il convient enfin d'évaluer les politiques comptables révélatrices d'anomalies pouvant découler de la fraude.

Comme la direction a le contrôle principal des activités commerciales, elle a le pouvoir d'établir et modifier les missions de contrôle y relatives. De ce fait, elle est en mesure d'outrepasser les contrôles pouvant entraîner des anomalies financières significatives. En réponse à ce risque de management override, l'auditeur doit examiner les écritures comptables principales effectuées de manière habituelle, mais aussi les écritures d'ajustement afin d'identifier des entrées inhabituelles, de fin de période, etc., et évaluer leur caractère éventuellement frauduleux. L'auditeur doit également estimer l'influence possible sur les estimations comptables et vérifier si elles sont raisonnables. À terme, l'auditeur doit décider si des procédures supplémentaires doivent être mises en œuvre pour répondre au risque de management override.

Vient ensuite la phase d'évaluation des éléments probants obtenus. L'auditeur doit examiner si les procédures analytiques mises en œuvre lors de la finalisation de la mission d'audit indiquent une fraude ou un risque non reconnu dans l'évaluation préliminaire. Lors de l'identification des anomalies, l'auditeur doit analyser si elles sont causées par une fraude ou une erreur. Si une anomalie est considérée comme résultant d'une fraude, l'auditeur doit, en fonction de l'importance des anomalies, déterminer l'évaluation des risques liés à la fraude et déterminer si des procédures complémentaires sont appropriées. L'auditeur doit également réexaminer les éléments probants déjà obtenus par la direction, car leur fiabilité peut en être affectée notamment par la collusion avec des employés et/ou des tiers.

L'auditeur doit tenir compte des implications sur l'audit et sur son rapport si :

- la fraude est confirmée;
- il n'est pas en mesure de confirmer si les anomalies significatives sont dues ou non à la fraude.

### 4.2.4. Incapacité de poursuivre la mission

Si l'auditeur n'est pas en mesure de continuer à travailler sur la mission à la suite d'une fraude, réelle ou suspectée, il doit veiller, d'une part, aux obligations qui lui sont imposées par la loi et la profession, y compris la communication de la question avec l'organe ayant nommé l'auditeur ou, dans certains cas, les autorités réglementaires. D'autre part, l'auditeur peut se retirer de l'engagement s'il le juge nécessaire et si les lois applicables dans le pays concerné l'y autorisent.

### 4.2.5. Communication

Comme indiqué précédemment, l'auditeur doit informer les responsables de la gouvernance ou le niveau de direction approprié de leurs responsabilités en matière de prévention et de détection des fraudes.

Lorsque l'auditeur identifie ou soupçonne une fraude, il doit le signaler sans délai à la direction à un niveau hiérarchique approprié. Si la fraude implique la direction ou un employé ayant une fonction déterminante dans le système de contrôle interne ou pouvant affecter les données financières, l'auditeur doit alors en informer les responsables de la gouvernance.

En outre, l'auditeur doit obtenir une déclaration écrite de la direction précisant qu'il incombe à cette dernière de concevoir et de mettre en œuvre un système de contrôle interne capable de prévenir et de détecter la fraude. Cette déclaration permet de confirmer plusieurs éléments :

- la direction a effectivement procédé à une évaluation selon laquelle les états financiers pourraient comporter des inexactitudes importantes en raison de fraudes;
- la divulgation de toute fraude réelle ou suspectée impliquant un employé, la direction ou un tiers;
- toute fraude ou allégation de fraude réelle ou présumée affectant les états financiers signalée par un employé, des analystes, les autorités ou autres.

Lorsqu'une fraude est découverte, l'entreprise a tendance à dissimuler la situation en écartant directement les personnes responsables ou en recouvrant les pertes par ses propres moyens. En général, les entreprises révèlent peu d'éléments pour préserver leur image auprès des tiers (Petraşcua & Tieanu, 2014).

Lorsque l'auditeur découvre ou suspecte une fraude, il doit vérifier, en fonction de la législation du pays, s'il est tenu de garder les informations du client confidentielles. En effet, dans certains pays, les obligations légales l'emportent sur cette obligation de secret professionnel. Les obligations spécifiques aux auditeurs belges en matière de dénonciation à la Cellule de Traitement des Informations Financières (CTIF) sont abordées au point suivant. De plus, l'article 86§1 de la loi du 7 décembre 2016 portant organisation de la profession et de la supervision publique des réviseurs d'entreprises prévoit certaines exceptions où le secret professionnel est levé.

Dans la documentation d'audit relative à la fraude, l'auditeur doit intégrer les éléments suivants:

- décisions importantes prises lors des discussions avec l'équipe de mission ;
- risque d'anomalies significatives provenant d'une fraude au niveau des états financiers et des assertions ;
- procédures réactives basées sur le risque évalué, c'est-à-dire leur nature, leur calendrier et leur étendue ;
- éléments de preuve obtenus grâce à l'application de ces procédures ;
- communication avec les responsables de la gouvernance, les autorités, les régulateurs, etc. ;
- justification de l'auditeur selon laquelle le risque de fraude dans la comptabilisation des produits n'est pas applicable dans le cadre de la mission.

### 4.2.6. Lutte contre le blanchiment d'argent et le financement du terrorisme

La loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces[26] modifie la loi du 11 janvier 1993. Elle a été adoptée suite à la quatrième directive européenne en matière de lutte contre le blanchiment d'argent et le financement du terrorisme et intègre les Normes internationales du Groupe d'action financière (GAFI).

L'article 67 de cette loi prévoit que le paiement ou le don en espèces est limité à maximum 3.000 EUR dans le cadre d'une opération ou d'un ensemble d'opérations qui semblent liées. Le

[26] Cfr annexe 2 : Communication 2017/15 de l'institut des reviseurs d'entreprises, page A3

non-respect de cette disposition est sanctionné par une amende allant de 250 à 225.000 EUR sans excéder 10 % du paiement ou du don dans le chef du vendeur et de l'acheteur.

Ici encore, l'évaluation des risques joue un rôle important puisque, en fonction de celle-ci, les réviseurs sont tenus d'adapter les mesures de prévention contre le blanchiment de capitaux et le financement du terrorisme (art.7).

En outre, tous les cabinets de révision, quelle que soit leur taille, doivent désigner une ou plusieurs personnes *(Compliance Officer)* dont la mission est de veiller à la mise en œuvre des mesures de contrôle interne. Le *Compliance Officer* est également tenu d'analyser les opérations jugées atypiques[27] pour vérifier si celles-ci sont liées au blanchiment de capitaux et du financement du terrorisme. Cette analyse doit ensuite faire l'objet d'un rapport spécial. S'il soupçonne que des opérations sont liées au blanchiment de capitaux ou au financement du terrorisme (art.47), le *Compliance Officer* a l'obligation d'informer la Cellule de Traitement des Informations Financières (CTIF).

[27] Les opérations atypiques sont des opérations qui sont soit anormalement complexes et d'un montant inhabituellement élevé, ou intrinsèquement inhabituelles, sans justification économique ou légitimité apparentes, soit incohérentes avec le profil du client. (*IRE - Communication 2017/15 : Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces).*

# Chapitre 5. Étude de cas

Ce chapitre présente le processus d'élaboration des méthodes de recherche et décrit la stratégie de collecte de données, y compris la sélection de l'instrument de recherche et de l'échantillonnage.

Les approches de recherche sont des plans d'action et des procédures comportant plusieurs étapes allant de la formulation d'hypothèses générales qui sous-tendent notre recherche aux méthodes de collecte de données, en passant par l'analyse et l'interprétation des résultats.

Les différentes décisions impliquées dans le processus sont utilisées afin de décider quelle approche devrait être utilisée dans le contexte spécifique d'une étude. Guetterman (2018) et Lewis (2015) soutiennent que la sélection d'une approche de recherche spécifique est basée sur la nature du problème de recherche, les expériences personnelles des chercheurs, et même le public pour lequel l'étude est développée.

Il existe de nombreuses façons de personnaliser les approches de recherche pour développer l'approche la plus appropriée pour une étude particulière. Les trois principales méthodes autour desquelles la recherche est organisée sont des méthodes qualitatives, quantitatives et mixtes.

Creswell (2013) fait remarquer que les trois approches ne doivent pas être considérées comme des catégories rigides, distinctes les unes des autres ou encore dichotomiques. Une étude « tend » à être plus quantitative que qualitative ou vice-versa. La recherche sur les méthodes mixtes est capable d'intégrer des éléments et caractéristiques des deux approches susmentionnées.

La principale distinction souvent citée entre les recherches quantitative et qualitative est que l'étude quantitative est formulée en termes d'utilisation de nombres plutôt que de mots, ou en utilisant des questions fermées pour les hypothèses quantitatives tandis que les entrevues qualitatives ont plutôt recours à des questions ouvertes. Tandis qu'une approche qualitative est couramment utilisée lorsqu'il y a peu ou pas de connaissance d'un phénomène.

Dans le cadre de cette étude, nous avons décidé d'adopter une approche mixte. Nous avons d'abord eu recours à une approche quantitative consistant à collecter des données numériques puis à les analyser afin d'expliquer un phénomène spécifique. Ensuite, nous avons utilisé l'approche qualitative afin d'affiner les résultats obtenus par voie quantitative.

## 5.1. Étude quantitative

Dans un premier temps, une enquête a été menée sur base d'un questionnaire. Lors de nos recherches, nous avons pu constater que la plupart des études présentes dans la littérature portent sur la fraude de façon globale, comme par exemple les différents sondages réalisés par de grands cabinets d'audit mentionnés précédemment. Notre étude concerne de façon plus précise le domaine de la fraude interne, car il y a moins d'analyses spécifiques réalisées à ce sujet. C'est pourquoi nous nous sommes inspirées pour notre étude quantitative d'une étude récente menée par Zager et al. (2016)[28].

### 5.1.1. Données et méthodologie

Il existe de nombreux instruments disponibles pour mettre en œuvre une étude quantitative. Chaque instrument présente ses avantages et inconvénients en termes de qualité, de temps et de coût de récolte des données. Saunder et Tosey (2013) indiquent que les données quantitatives récoltées par voie de questionnaires sont plus simples à obtenir et plus concises à présenter. Les enquêtes sont considérées comme la forme de recherche la plus traditionnelle et utile en matière de processus descriptif non expérimental qui cherche à décrire une certaine forme de réalité. Les questionnaires sont souvent limités à un échantillon représentatif d'un groupe potentiel représentant l'intérêt de l'étude.

Par conséquent, nous avons opté pour une enquête en ligne grâce à l'outil « Google Forms ». Un questionnaire[29] a été proposé afin de recueillir des données exploitables concernant une information financière frauduleuse au sein d'entreprises belges.

L'échantillon de répondants à ce questionnaire se compose d'auditeurs externes et de réviseurs d'entreprises faisant partie du tissu économique belge wallon. Un mail a été envoyé à toute une série de contacts. Ceux-ci proviennent du site de l'Institut des Réviseurs d'Entreprises (IRE) qui répertorie l'ensemble des réviseurs belges dans le registre public. Dans le cadre de notre stage, nous avons également pu obtenir d'autres contacts. Une centaine de mails ont pu être envoyés.

---

[28] Zager, L., Sever Malis, S., & Novak, A. (2016). The role and responsibility of auditors in prevention and detection of fraudulent financial reporting. *Procedia Economics and Finance*, *vol.*39, 693-700. doi: 10.1016/S2212-5671(16)30291-X.

[29] Cfr annexe 3 : Étude quantitative, page A9

Dans la première partie du questionnaire, il a été demandé aux intervenants de fournir des informations sur des cas de fraude qui leur sont familiers et d'évaluer la fréquence à laquelle ils ont fait face à des circonstances pouvant indiquer une possibilité de fraude. Les situations qui leur ont été soumises, reprises ci-dessous, sont formulées sur base de la Norme Internationale d'Audit 240 – Responsabilités de l'auditeur en matière de fraude dans un audit des états financiers. Les circonstances qui y sont mentionnées sont classifiées en quatre groupes. Nous les avons simplifiées et adaptées à l'échelle de l'étude.

**Situation 1** Des opérations incorrectement enregistrées (pas totalement enregistrées, pas en temps voulu ou pour un montant erroné, dans la mauvaise période ou le mauvais compte ou en contradiction avec les règles d'évaluation de l'entité).

**Situation 2** Des ajustements de dernière minute qui affectent les résultats de manière significative.

**Situation 3** Des affirmations ou des plaintes auprès de l'auditeur concernant des fraudes alléguées.

**Situation 4** Des documents qui semblent avoir été altérés.

**Situation 5** Des différences inhabituelles entre la comptabilité de l'entité et les réponses reçues aux demandes de confirmations externes.

**Situation 6** Un plus faible taux de réponse aux demandes de confirmations externes que celui attendu ou, au contraire, un taux beaucoup plus élevé.

**Situation 7** La pression excessive, en termes de délai, exercée par la direction pour résoudre des questions complexes ou des sujets contentieux.

**Situation 8** Des plaintes de la direction concernant la façon dont l'audit se déroule, ou la volonté de la direction d'intimider les membres de l'équipe affectée à la mission.

**Situation 9** Une lenteur inhabituelle de l'entité à fournir les informations demandées.

**Situation 10** La réticence de la direction à amender ou à réviser les informations fournies dans les états financiers pour les rendre plus complètes ou plus explicites.

**Situation 11** La réticence de la direction à entreprendre des actions en temps voulu liées aux faiblesses du contrôle interne identifiées.

**Situation 12** Le fait que des entorses au code de conduite de l'entité soient tolérées.

Nous avons fait appel à l'échelle de Likert (parfois/souvent/très fréquemment) permettant d'évaluer la fréquence à laquelle les répondants ont rencontré certains mécanismes pouvant indiquer une fraude.

Dans le cadre de l'enquête, il a également été demandé aux auditeurs de juger, selon leur opinion et leur expérience, l'efficacité de certaines mesures spécifiques de prévention de la fraude :

- contrôle interne ;
- mise en place d'une ligne téléphonique ;
- code de conduite ;
- environnement de travail ne tolérant aucun comportement frauduleux ;
- formations pour sensibiliser les cadres et les employés.

Nous avons également interrogé les répondants sur leur utilisation des outils d'analyse de données :

- analyse des ratios financiers ;
- arbres de décision ;
- text mining ;
- méthode SVM (Support Vector Machine) ;
- loi de Benford.

La dernière partie du questionnaire consistait à solliciter auprès des participants quelques informations personnelles telles que le sexe, l'âge, le titre, le nombre d'années d'expérience et la taille du cabinet d'audit dans lequel ils exercent.

L'objectif de cette étude est de rassembler des informations sur les types de transactions vulnérables pouvant constituer une information financière frauduleuse et obtenir l'avis des auditeurs et réviseurs interrogés sur certaines mesures de prévention à mettre en place dans les entreprises ainsi que sur les différents outils de détection qu'ils utilisent.

### 5.1.2. Hypothèses

Sur base de notre revue de littérature et plus particulièrement des enquêtes menées par de grands cabinets, nous nous attendons à ce que plus de 50 % des répondants aient déjà découvert un cas de fraude au cours d'un audit. De plus, si nous nous basons sur les statistiques de fraude, les détournements d'actifs devraient représenter la majeure partie des cas rencontrés.

Nous avons conscience que les douze situations proposées issues de la norme d'audit 240 constituent toutes des *indices* de fraude. Dans la pratique, les auditeurs et réviseurs d'entreprises sont donc susceptibles de les rencontrer sans pour autant qu'elles ne révèlent une fraude. Le but sera donc de relever les situations pour lesquelles les avis sont partagés et obtenir des explications au travers des interviews réalisées dans le cadre de l'étude qualitative.

En supposant que chacune des mesures de prévention proposées est mise en place de manière optimale au sein des entreprises, nous pouvons raisonnablement penser, sur base de notre revue de la littérature, qu'elles constituent toutes un moyen efficace de lutter contre la fraude. Toutefois, selon l'expérience professionnelle des répondants, nous pourrons mettre en avant les mesures de protection qui semblent les plus appropriées dans la lutte contre la fraude interne.

Enfin, d'après ce que nous avons constaté lors de nos stages respectifs, nous émettons l'hypothèse que l'analyse des ratios financiers et la loi de Benford sont les outils les plus utilisés par les professionnels et que la méthode SVM (Support Vector Machine), le text mining et les arbres de décision sont un peu moins connus, surtout dans les plus petites structures.

### 5.1.3. Analyse des résultats

Nous avons récolté les résultats du questionnaire entre le 13 mars et le 17 avril 2020. L'ensemble des résultats de l'étude quantitative figurent à l'annexe 4, page A19.

Nous avons obtenu 48 réponses sur une centaine de mails envoyés. Si le taux de réponse n'avait pas été satisfaisant, nous aurions pris la décision d'étendre l'étude auprès des réviseurs néerlandophones.

Il est intéressant de noter que 56,3 % des personnes interrogées possèdent le titre de réviseur d'entreprises. La plupart des répondants sont des hommes (77,1 %), ceci s'expliquant par la répartition par genre au sein de l'Institut des Réviseurs d'Entreprises (IRE) constitué à 71 % d'hommes.

Le panel est suffisamment diversifié au niveau des tranches d'âge. En effet, des personnes de tout âge ont répondu au questionnaire, les tranches des 20-29 et des 30-39 étant majoritaires (figure 14). Ce résultat n'est pas représentatif de l'ensemble de la profession[30], mais plus de la moitié des personnes ayant entre 20 et 39 ans ont plus de cinq ans d'expérience dans l'audit.

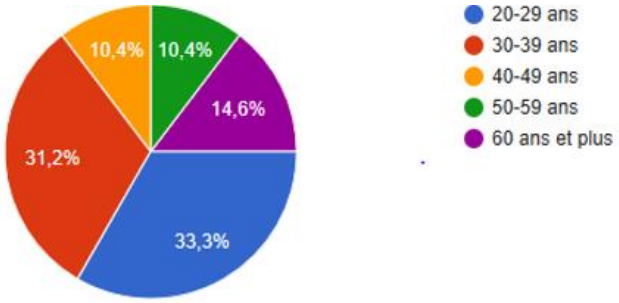



*Figure 14: Résultats de l'étude quantitative (annexe 4, page A19)*

Parmi les 48 intervenants, 25 travaillent dans un cabinet de taille moyenne à grande, 13 proviennent d'un petit cabinet, 6 travaillent dans un Big Four et 4 travaillent seuls. Il est à préciser que 75 % des répondants ont plus de 5 ans d'expérience dans le domaine de l'audit, ce qui rend les résultats pertinents.

La première partie du questionnaire porte sur la fraude. À la question « Avez-vous déjà découvert un cas de fraude au cours d'un audit », 64,6 % des participants affirment avoir été confrontés à un cas de fraude lors d'un audit. Parmi ces réponses, la fraude la plus courante consiste au détournement d'actifs.

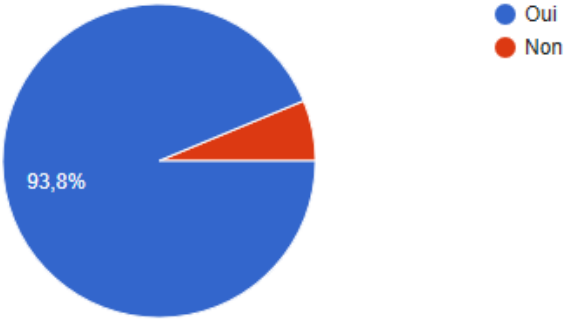
Parmi les douze situations reprises de la norme internationale d'audit 240 pouvant indiquer la possibilité que les états financiers comportent des anomalies significatives provenant de fraudes, trois situations récoltent le plus de réponses :

[30] IRE (2019). *La profession*. En ligne https://2019.rapportannuelire.be, consulté le 11 mai 2020.

SITUATION : Des ajustements de dernière minute qui affectent les résultats de manière significative.

Cette situation constitue-t-elle pour vous un risque de fraude ?

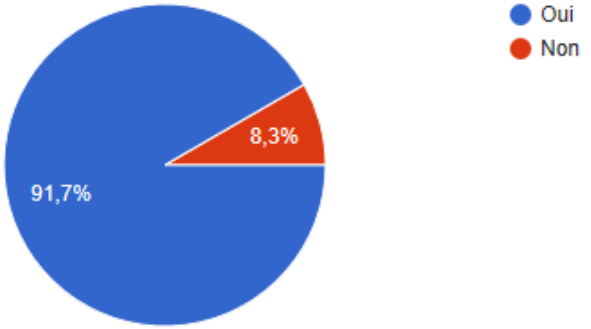
45 réponses




SITUATION : Des affirmations ou des plaintes auprès de l'auditeur concernant des fraudes alléguées.

Cette situation constitue-t-elle pour vous un risque de fraude ?

44 réponses




SITUATION : Des documents qui semblent avoir été altérés.

Cette situation constitue-t-elle pour vous un risque de fraude ?

43 réponses

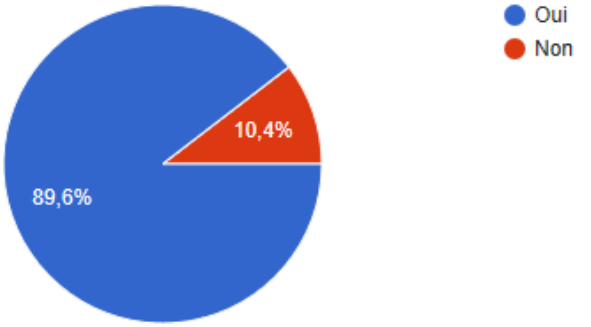



*Figure 15: Résultats de l'étude quantitative (annexe 4, page A19)*

Concernant les ajustements de dernière minute, 34 répondants parmi les 45 ont déjà rencontré ce type de situation, dont 27 ont répondu « parfois » à la question de la fréquence. Environ la moitié des personnes considérant les deuxième et troisième situations comme risquées indiquent les avoir rencontrées parfois.

Nombreux sont ceux qui ont noté les situations suivantes comme risquées :

- des opérations incorrectement enregistrées (40 réponses) ;
- le fait que des entorses au code de conduite de l'entité soient tolérées (40 réponses) ;
- des plaintes de la direction concernant la façon dont l'audit se déroule, ou la volonté de la direction d'intimider les membres de l'équipe affectée à la mission (39 réponses) ;
- la réticence de la direction à entreprendre des actions en temps voulu liées aux faiblesses du contrôle interne identifiées (39 réponses) ;
- la pression excessive, en termes de délai, exercée par la direction pour résoudre des questions complexes ou des sujets contentieux (37 réponses) ;
- des différences inhabituelles entre la comptabilité de l'entité et les réponses reçues aux demandes de confirmations externes (34 réponses).

Seules 10 personnes sur 40 indiquent avoir rencontré des entorses au code de conduite tolérées par l'entité.

Pour deux autres situations, les avis sont partagés. La moitié des intervenants estime qu'une lenteur inhabituelle de l'entité à fournir les informations demandées ainsi que la réticence de la direction à réviser les informations fournies dans les états financiers pour les rendre plus complètes ou explicites ne constituent pas un risque de fraude.

Enfin, seulement 22,9 % des personnes interrogées estiment qu'un plus faible taux de réponse ou, au contraire, un taux beaucoup plus élevé de confirmations externes que celui attendu constitue un risque de fraude.

Dans la seconde partie du questionnaire, il a été demandé aux répondants d'évaluer, selon leur jugement professionnel l'efficacité de certaines mesures de prévention sur l'échelle de Likert de 0 à 4 (1 signifie extrêmement inefficace et 4 signifie extrêmement efficace). Le tableau repris ci-dessous montre que les mesures de prévention efficaces sont, par ordre d'importance, un environnement de travail ne tolérant aucun comportement frauduleux (moyenne pondérée :

3,19), un contrôle interne (moyenne pondérée : 2,92), des formations (moyenne pondérée : 2,79), un code de conduite (moyenne pondérée : 2,33) et enfin une ligne téléphonique (moyenne pondérée : 1,60).

| Mesures de prévention | 0 | 1 | 2 | 3 | 4 | Moyenne pondérée |
|---|---|---|---|---|---|---|
| Contrôle interne | 0 | 1 | 11 | 27 | 9 | 2,92 |
| Ligne téléphonique | 13 | 9 | 13 | 10 | 3 | 1,60 |
| Code de conduite | 2 | 5 | 18 | 21 | 2 | 2,33 |
| Environnement de travail ne tolérant aucun comportement frauduleux | 0 | 3 | 7 | 16 | 22 | 3,19 |
| Formations pour sensibiliser les cadres et les employés | 2 | 1 | 10 | 27 | 8 | 2,79 |

*Tableau 3: Résultats de l'enquête quantitative (annexe 4, page A19)*

Enfin, nous avons identifié les outils d'analyse de données utilisés par les auditeurs et les réviseurs d'entreprises. Selon le schéma repris ci-dessous, les outils les plus exploités sont l'analyse des ratios financiers (45 réponses), suivie des arbres de décision (29 réponses), de la loi de Benford (28 réponses), de la technique du text mining (14 réponses) et de la méthode Support Vector Machine (5 réponses). Certains ont mis en évidence d'autres outils d'analyse tels que des outils développés en interne afin de revoir les combinaisons d'écritures, les transactions inhabituelles, etc.

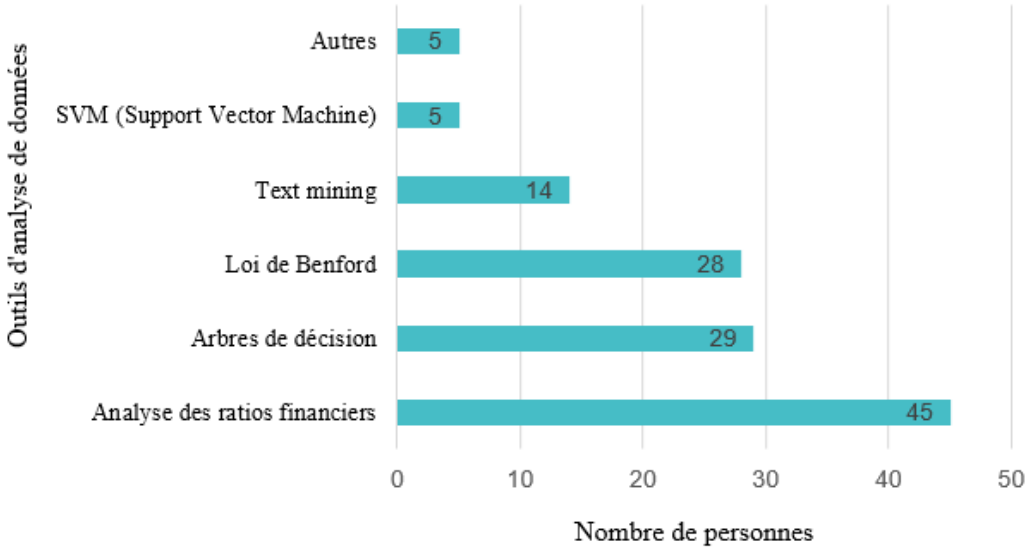



*Figure 16: Résultats de l'étude quantitative (annexe 4, page A19)*

Il est important de noter que dans le cadre de cette étude, une analyse statistique des résultats obtenus n'est pas pertinente. En effet, le type de réponses obtenues (réponses de type oui-non) dans le sondage ne se prête pas à une telle analyse. De plus, le nombre de réponses enregistrées (48 réponses) n'est pas suffisant pour atteindre des résultats statistiquement fiables. Il est à préciser que le modèle d'étude[31] sur lequel nous nous sommes basées ne reprend pas une analyse statistique.

## 5.2. Étude qualitative

Comme mentionné précédemment, nous avons choisi d'avoir recours à une approche mixte. Dans un premier temps, une enquête quantitative a été menée afin de collecter des données sur la problématique envisagée. Dans un second temps, une étude qualitative a été réalisée afin d'affiner ces résultats.

### 5.2.1. Données et méthodologie

Harrell et Bradley (2009) indiquent que la recherche qualitative est un type de recherche scientifique. De manière générale, la recherche scientifique consiste en une enquête qui :

- cherche des réponses à une question de recherche ;
- utilise systématiquement un ensemble de procédures prédéfinies pour répondre à la question de recherche ;
- recueille des preuves ;
- produit des résultats qui n'ont pas été déterminés à l'avance ;
- produit des résultats qui sont applicables au-delà des limites immédiates de l'étude.

La recherche qualitative possède ces caractéristiques. En outre, elle tente de comprendre un problème de recherche donné, à partir du point de vue de la population étudiée. La recherche qualitative est donc particulièrement efficace pour obtenir des informations spécifiques sur des opinions, comportements et contextes sociaux particuliers.

[31] Zager, L., Sever Malis, S., & Novak, A. (2016). The role and responsibility of auditors in prevention and detection of fraudulent financial reporting. *Procedia Economics and Finance*, *vol.*39, 693-700. doi: 10.1016/S2212-5671(16)30291-X.

Lorsqu'elle est combinée avec des méthodes quantitatives, la recherche qualitative aide à mieux comprendre la réalité d'une situation donnée et à interpréter les implications des données quantitatives obtenues. Les résultats peuvent souvent être étendus à d'autres personnes ayant des caractéristiques similaires à celles de la population étudiée.

Les trois méthodes qualitatives les plus courantes sont l'observation des participants, les entretiens approfondis et les groupes de discussion. Dans le cadre de notre étude, nous avons choisi de mener des entretiens individuels avec des auditeurs et des réviseurs d'entreprises. Ces interviews sont efficaces pour collecter des données sur les expériences et les perspectives professionnelles.

Les entretiens peuvent être placés sur une échelle de structure allant de « non directif » à « directif ». Il ressort de cette notion d'échelle l'idée du degré de contrôle que peut avoir l'interviewer sur l'interaction. Notre souhait étant d'approfondir le sujet et d'obtenir des explications sur les réponses fournies lors de l'étude quantitative, l'entretien de type semi-directif semble le plus approprié. Celui-ci nous permet d'avoir une certaine liberté d'action quant à l'ordre dans lequel les questions prédéfinies sont posées. Nous avons donc élaboré un guide d'entretien[32] afin de mener à bien nos interviews. Ce dernier se compose des points principaux suivants :

- présentation de l'étude ;
- présentation du répondant ;
- questions relatives au contrôle interne ;
- outils de prévention/détection de la fraude ;
- discussion relative aux résultats de l'enquête quantitative ;
- remerciements.

Bien que cette démarche reste faisable, il n'est pas nécessaire de collecter des données auprès de tous les membres d'une communauté afin d'obtenir des résultats valides, dans notre cas les 48 répondants au questionnaire quantitatif. Dans la recherche qualitative, seul un échantillon d'une population est sélectionné pour une étude donnée. Les objectifs de recherche ainsi que les

[32] Cfr annexe 5 : Guide d'entretien, page A38

caractéristiques de taille et de diversité déterminent qui et combien de personnes seront sélectionnées.

Lors de l'étude quantitative, les répondants ont eu la possibilité de communiquer leur numéro de téléphone ou leur adresse mail en vue de participer éventuellement à un entretien individuel. 19 personnes ont laissé leurs coordonnées.

Vu le confinement imposé suite à la pandémie du Covid-19, nos entretiens ont été réalisés à distance (Skype, appel téléphonique) auprès de cinq réviseurs d'entreprises faisant partie des plus grands cabinets d'audit :

- Jean-François Bernard, senior manager (BDO Liège)[33] ;
- Amandine Desmedt, réviseur d'entreprises (Ernst & Young)[34] ;
- Thomas Meurice, réviseur d'entreprises et Directeur (PwC)[35] ;
- Marie Delacroix, réviseur d'entreprises (RSM InterAudit)[36] ;
- Patricia Leleu, réviseur d'entreprises (KPMG)[37].

Leurs années d'expérience dans le domaine de l'audit varient de six ans et demi à trente ans. Il est important de signaler que nous avons réussi à entrer en contact avec l'un des membres du département Forensic & Litigation Services de BDO.

### 5.2.2. Analyse des interviews

Jean-François Bernard, senior manager chez BDO, estime qu'un contrôle interne pertinent permet de prévenir la fraude. Cependant, selon lui, il est très rare qu'il soit conçu sans faille et appliqué de manière permanente. Par exemple, il constate dans les entreprises que le cycle d'achat est souvent bien conçu en termes de séparation des fonctions, mais à l'inverse, très peu de contrôle sont mis en place pour les notes de crédit sur vente. Selon Thomas Meurice, directeur chez PwC, une entreprise peut avoir les meilleurs contrôles mis en place mais si la séparation de fonctions n'est pas respectée, le risque de fraude est bien présent. Amandine

[33] Cfr annexe 6 : Interview de Jean-François Bernard, page A41
[34] Cfr annexe 7 : Interview de Amandine Desmedt, page A51
[35] Cfr annexe 8 : Interview de Thomas Meurice, page A59
[36] Cfr annexe 9 : Interview de Marie Delacroix, page A64
[37] Cfr annexe 10 : Interview de Patricia Leleu, page A69

Desmedt, réviseur d'entreprises au sein du cabinet Ernst & Young, ainsi que Marie Delacroix, réviseur d'entreprises pour RSM, partagent cet avis. Amandine Desmedt précise qu'il est nécessaire de garder à l'esprit que le tissu économique belge est constitué aussi de plus petites structures où une telle séparation des fonctions est plus complexe à mettre en place. Elle rappelle aussi que le niveau hiérarchique où la fraude survient revêt une certaine importance. En effet, lorsque celle-ci est commise au niveau du management, des mécanismes peuvent être mis en place afin d'outrepasser le contrôle interne. Marie Delacroix, quant à elle, souligne l'importance de la réévaluation fréquente des procédures de contrôle interne afin de s'assurer que cet outil soit optimal dans le cadre de la prévention de la fraude. Patricia Leleu, associée au sein du cabinet KPMG, rappelle que le contrôle interne permet de limiter drastiquement le risque de fraude mais ne peut en aucun cas l'éliminer complètement. Si la fraude implique une collusion entre deux ou plusieurs personnes, les contrôles mis en place peuvent être contournés.

Le référentiel COSO apporte les lignes directrices à mettre en place en matière de contrôle interne. Les répondants ont proposé quelques améliorations qui pourraient être apportées à cet outil. Thomas Meurice déclare que le référentiel COSO est très peu connu par les entreprises et devrait être appliqué dans toutes les organisations. En revanche, Amandine Desmedt se questionne sur le caractère adapté de ce référentiel à des organisations de type PME telles que nous les connaissons en Belgique. Il existe une problématique de taille des structures mais aussi de culture. En effet, la Belgique ne disposerait pas d'une perception du contrôle interne ancrée dans les esprits comme c'est le cas aux États-Unis ou en France par exemple. Bon nombre d'entreprises familiales fonctionnent « à la confiance » et ne sont pas conscientes de l'éventualité qu'une personne mal intentionnée puisse commettre une fraude. Par facilité, bon nombre de petites structures préfèrent aussi un contrôle interne moins contraignant, les procédures d'approbation et de vérification ralentissant considérablement le processus d'achat ou de vente. Pour Marie Delacroix, il est nécessaire qu'un modèle COSO réorienté IT soit étudié en raison de l'évolution technologique de la fraude. Bien que les concepts généraux restent d'actualité, des spécifications orientées vers la cybercriminalité devraient voir le jour.

Les résultats de l'enquête ont permis de dégager une tendance. Selon les répondants, pour lutter contre la fraude, un environnement de travail ne tolérant aucune fraude se révèlerait être très efficace. Selon Jean-François Bernard, ne tolérer aucune fraude est indispensable, voire élémentaire, mais imposer uniquement cette mesure ne permettra pas de prévenir la fraude. Thomas Meurice affirme qu'il s'agit d'une mesure efficace mais est conscient qu'il existera

toujours des moyens pour commettre une fraude. Pour Marie Delacroix, il s'agit d'un axe très important. À partir du moment où une fraude, aussi minime soit-elle, est tolérée, cela démontre une faille dans le système. Il est donc indispensable que les contrevenants soient réprimandés et que cette réprimande soit connue du reste du personnel. Patricia Leleu partage cette opinion en soulignant qu'il s'agit d'une question de « tone at the top » qui donne la ligne directrice d'une organisation.

Les types de fraude les plus fréquents semblent être les détournements d'actifs qui, par exemple, consistent à utiliser l'argent de l'entreprise pour des besoins personnels. Amandine Desmedt met en évidence l'importance de rester attentif aux reclassements des montants dans certaines rubriques comptables dans le but d'améliorer les ratios financiers.

En ce qui concerne les outils de détection de la fraude utilisés, il s'agit notamment d'outils d'analyse de données permettant de repérer des transactions particulières. Quatre répondants ont déjà eu recours à la loi de Benford mais deux d'entre eux considèrent que cet outil est un peu trop scolaire et n'est pas efficace dans la détection de la fraude. Trois réviseurs d'entreprises ont déjà employé la technique du text mining. Les méthodes SVM et les arbres de décision sont moins connus, une seule personne interviewée indique les employer. À noter qu'en réponse à cette question, une répondante a souligné que selon la norme ISA 240, l'auditeur n'a pas une obligation de détection de la fraude mais plutôt une obligation d'évaluation du risque de fraude.

Dans le cas d'une fraude suspectée, les répondants n'utilisent pas d'autres outils en particulier. Si la fraude est significative, des tests complémentaires sont effectués (tests d'échantillonnage) afin de s'assurer qu'il n'y a pas eu de fraude dans d'autres rubriques. Des questions se posent : « Peut-on faire confiance aux résultats de l'audit ? » ou encore « Doit-on revoir la matérialité à la baisse pour l'ensemble de l'audit ? ». Marie Delacroix souligne que l'emploi des data analytics permet d'identifier des informations suspectes et d'analyser toutes les opérations y relatives puisqu'en matière de fraude, il n'y a pas de seuil de signification ou de matérialité.

Selon les résultats de notre étude quantitative, les formations sont efficaces pour prévenir la fraude. Pourtant, Jean-François Bernard, membre du département Forensic & Litigation de BDO qui propose des services de formation contre la fraude aux entreprises, ne suit pas cet avis. Il trouve les formations très théoriques et ne souhaite pas promouvoir ce type de service. Thomas Meurice estime que les formations n'empêchent pas les membres du personnel de frauder et qu'il y aura toujours un risque que les contrôles mis en place soient outrepassés. Par

contre, selon Amandine Desmedt, ce type de formation permet de conscientiser les entreprises sur l'importance du contrôle interne. Cette démarche permet d'ouvrir la réflexion avec le client sur la nécessité de mettre en place des mécanismes prévenant la fraude avant que celle-ci n'ait lieu. Patricia Leleu, quant à elle, considère qu'en fonction de la spécificité de chaque entreprise, les formations efficaces sont celles qui mettent en avant des cas concrets et qui sont liées à des procédures en vigueur sur le terrain afin de véhiculer un message fort.

Selon les résultats de l'enquête quantitative, la majorité des répondants de l'étude quantitative estime que la ligne téléphonique de dénonciation n'est pas vraiment une mesure de prévention efficace contre la fraude. L'une des personnes interviewées, Jean-François Bernard, a l'impression que ce n'est pas vraiment dans la mentalité des gens de dénoncer un comportement frauduleux. Cependant, suite à une nouvelle directive européenne qui rentrera en application en décembre 2021, certaines entreprises devraient être intéressées par ce procédé. Son équipe a d'ailleurs l'intention de développer ce service étant donné que leurs missions débutent généralement par une dénonciation anonyme. Les interviews montrent que les avis sont partagés sur la question. D'une part, les répondants pensent que la délation n'est pas répandue dans nos coutumes, mais d'autre part, ce système pourrait être efficace. Patricia Leleu est d'avis que cet outil pourrait démontrer son utilité dans les cas de fraude relatifs au reporting financier où des employés sont soumis à une pression importante de la part de la direction.

Les résultats de l'enquête quantitative indiquent l'utilisation de ratios financiers comme principal outil d'analyse de données. Jean-François Bernard insiste sur le fait qu'il faut avoir des ratios très précis. Deux répondants estiment que des ratios financiers généraux tels que le ratio de solvabilité ou le ratio de liquidité ne permettraient pas de mettre en évidence un cas de fraude sauf si le préjudice subi par l'entreprise est considérable par rapport au chiffre d'affaires réalisé. Selon eux, la fraude s'identifie rarement au travers de ratios. Pour Marie Delacroix, ce n'est pas le ratio en lui-même qui importe, mais plutôt la comparaison avec le ratio de l'année précédente ou le ratio du secteur ou encore le ratio d'un concurrent. Néanmoins, selon Amandine Desmedt, l'auditeur doit rester vigilant à la situation spécifique dans laquelle se trouve l'entreprise auditée. Une société communiquant, par exemple, sur son EBITDA ou sur certains ratios permettant de maintenir son investissement à long terme pourrait être tentée de manipuler ces informations. Selon Patricia Leleu, les ratios de cash-flow et de trésorerie se révèlent fort intéressants pour identifier les manipulations comptables. Ces derniers permettent

de mettre en évidence une amélioration du chiffre d'affaires et du résultat ne se traduisant pas par une amélioration de la trésorerie.

Ont été reprises dans l'enquête en ligne douze situations issues de la norme internationale d'audit 240 pouvant indiquer la possibilité que les états financiers comportent des anomalies provenant de fraudes. Pour deux situations, les avis sont partagés.

Concernant la première situation, la moitié des répondants de l'étude quantitative estime qu'une lenteur inhabituelle de l'entité à fournir les informations demandées constitue un risque de fraude. Selon Jean-François Bernard, une lenteur inhabituelle peut provenir d'un retard dans la finalisation des comptes à cause d'un manque d'effectifs dans les entreprises ou bien des mesures actuelles concernant le Covid-19. Dans ces cas-là, il ne s'agit pas forcément d'un risque de fraude. En revanche, une entreprise qui habituellement, finalise ses comptes quinze jours après la date de clôture et qui tout à coup a besoin de cinquante jours pour les clôturer peut être considérée comme suspecte. Thomas Meurice constate que les entreprises qui délivrent tardivement les informations demandées sont en manque d'effectifs ou emploient du personnel qui n'est pas forcément compétent dans ce domaine pour délivrer des informations correctes. Cependant, il est vrai qu'une information anormalement tardive ou « brouillon » pourrait être un indicateur de fraude.

La deuxième situation porte sur la réticence de la direction à réviser les informations fournies dans les états financiers pour les rendre plus complètes ou explicites. Jean-François Bernard estime qu'il s'agit d'une situation trop générale. Il est nécessaire de se demander quel serait l'intérêt de la direction à manipuler les états financiers et analyser si l'ajustement est matériel ou non. Par exemple, pour montrer ses comptes sous leur plus beau jour, une entreprise a tendance à gonfler ses résultats. Si l'ajustement proposé par le réviseur d'entreprises est matériel et peut empêcher l'entreprise de présenter le résultat souhaité, cette situation peut être considérée comme un indicateur de fraude. Thomas Meurice apporte l'exemple d'une entreprise qui ne souhaite pas effectuer l'ajustement demandé, car celui-ci n'est pas matériel pour la comptabilité du groupe. Dans ces conditions, il ne s'agit pas d'un cas de fraude, car l'entreprise décide de privilégier les comptes de la maison mère.

Dans le cadre de l'étude quantitative, seulement 22,9 % des personnes interrogées estiment qu'un plus faible taux de réponse ou, au contraire, un taux beaucoup plus élevé de confirmations externes que celui attendu constitue un risque de fraude. Jean-François Bernard trouve judicieux

de se demander s'il s'agit d'un taux plus faible ou plus élevé par rapport à la moyenne des autres clients ou par rapport au taux historique du client. Selon lui, se baser sur la moyenne n'a aucun sens, car le taux de réponse varie en fonction des entreprises. Par exemple, un client qui travaille avec des entreprises internationales risque d'avoir un taux de réponse beaucoup plus faible. Il serait donc peut-être plus pertinent de se baser sur le taux de réponse initial du client. De plus, Jean-François Bernard ajoute que les courriers de confirmation de solde doivent être envoyés par les réviseurs d'entreprises pour s'assurer que tous les courriers ont été envoyés. Thomas Meurice a rencontré le cas d'un client qui a obtenu 100 % de réponses aux demandes de confirmation. Il s'est avéré qu'un client extérieur signait toutes les lettres sans effectuer de vérification. Cela n'indique pas pour autant un cas de fraude, mais démontre plutôt les limites de la circularisation. Amandine Desmedt souligne que dans le cas d'une absence de réponse à la circularisation, des procédures alternatives sont mises en place pour la vérification des différents soldes. Le but premier de la confirmation n'est pas de valider l'exhaustivité, mais bien l'existence.

## 5.3. Synthèse des études quantitative et qualitative

Les éléments essentiels qui ressortent des études quantitative et qualitative sont :

- Plus de la moitié des réviseurs d'entreprises et des auditeurs externes interrogés ont déjà rencontré un cas de fraude au cours d'un audit.

- Ces cas de fraude concernaient principalement des détournements d'actifs.

- Pour deux situations parmi les douze proposées pouvant indiquer la possibilité que les états financiers comportent des anomalies provenant de fraudes, les avis sont partagés :

    - une lenteur inhabituelle de l'entité à fournir les informations demandées ;
    - la réticence de la direction à réviser les informations pour les rendre plus complètes et explicites.

    Ces situations doivent être analysées au cas par cas.

- Pour la majorité des répondants, la situation selon laquelle un plus faible taux de réponse ou, au contraire, un taux beaucoup plus élevé de confirmations externes que celui attendu ne constituerait pas systématiquement un risque de fraude.

- Parmi les mesures de prévention proposées, la plus efficace semble être un environnement de travail ne tolérant aucun comportement frauduleux. La direction montre l'exemple en prenant des mesures appropriées en cas de fraude afin de dissuader les éventuels fraudeurs.

- Le contrôle interne conçu de manière pertinente constitue également une mesure de prévention efficace contre la fraude interne.

- Plusieurs pistes d'amélioration pourraient être apportées par rapport au référentiel COSO :

  - l'application obligatoire de ce référentiel dans toutes les entreprises ;
  - l'intégration de spécifications orientées vers la cybercriminalité ;
  - une adaptation à la structure des petites entreprises.

- Les formations visant à prévenir la fraude en entreprise devraient être spécifiques à chaque entreprise et porter sur des cas concrets.

- La mise en place d'une ligne téléphonique d'urgence en tant que mesure de prévention ne fait pas l'unanimité.

- Les outils d'analyse de données les plus exploités sont l'analyse des ratios financiers, les arbres de décision et la loi de Benford. La méthode SVM et le text mining sont un peu moins connus, mais sont toutefois utilisés par quelques personnes.

# Chapitre 6. Fraude et actualité

Depuis son apparition fin 2019, le Covid-19 a entraîné la mort de plusieurs dizaines de milliers de personnes à travers le monde et, selon les experts, engendrera une crise économique sans précédent. La plupart des pays ont été contraints de prendre des mesures drastiques pour éviter au maximum la propagation du virus, notamment le confinement des populations. Toutes ces dispositions ne sont pas sans conséquence et impactent tous les secteurs. Une note d'information de l'ICCI parue le 31 mars 2020[38] indique un risque accru de fraude dans le contexte actuel d'audit à distance.

## 6.1. Impact sur le risque de fraude

Il existe une corrélation importante entre le risque de fraude et un dysfonctionnement du contrôle interne d'une part et un risque accru d'une mauvaise représentation du bilan d'autre part. Cette dernière peut être la résultante d'une volonté de la direction de masquer une rentabilité périclitante ou encore la nécessité de respecter les conventions préétablies.

Lors de la phase d'évaluation du risque, il est important de porter une attention toute particulière à la présence d'opportunités facilitant la fraude, à l'existence d'éventuelles pressions ainsi qu'à la possibilité de justification d'un tel acte. Il s'agit de la théorie du triangle de la fraude abordée précédemment.

Notons que le risque de fraude est considérablement accru au sein d'un environnement de contrôle interne affaibli. Ce dernier constitue le pilier « opportunité » du triangle de la fraude. L'absence de mesures de contrôle performantes offre la possibilité d'abuser de l'organisation.

En cette période de crise du Covid-19, les procédures de contrôle interne étant affaiblies, des opportunités de fraude se créent. Il est donc primordial de redoubler de vigilance.

[38] ICCI. (2020). FAQ COVID-19 : impact sur le contrôle interne et le risque de fraude et audit à distance. En ligne https://www.icci.be/fr/actualit/actualit-detail-page/faq-covid-19-impact-sur-le-contr-le-interne-et-le-risque-de-fraude-et-audit-distance?fbclid=IwAR2TOF9B3YFUxvmP6gGwI2f5-WK8iY5iz4ZqIephluLkb6E-DeORn1jE3AE, consulté le 6 avril 2020.

## 6.2. Impact sur le contrôle interne

Différents aspects découlant de la crise du coronavirus pourraient impacter le contrôle interne.

Tout d'abord, il se pourrait que les mesures de contrôle ne soient pas optimales en raison de la réduction du nombre de collaborateurs ou encore de la fermeture des bureaux. Il convient donc de procéder à une évaluation de ces contrôles dans pareil contexte.

Ensuite, la séparation des fonctions pourrait être rompue. En effet, une communication déficiente peut avoir des conséquences sur la séparation des fonctions au sein des organisations d'une part et sur les mesures de contrôles établies par la direction d'autre part. Dans le cas où les contrôles existants ne seraient plus pertinents, des contrôles alternatifs devront être en mesure de contrebalancer l'insuffisance d'informations.

Le troisième aspect repose sur l'affaiblissement éventuel des procédures d'autorisation. Effectivement, le travail à distance impliquant une modification des accès informatiques, une adaptation des contrôles existants doit être envisagée.

Il est à noter que le recours aux outils informatiques comporte également certains risques. Il s'agit notamment de la capacité du système à supporter une utilisation accrue. C'est pourquoi la robustesse de l'infrastructure informatique doit être testée et des solutions adéquates doivent être envisagées.

Dernier point, la capacité de la direction à clôturer le processus d'élaboration de l'information financière peut temporairement faire défaut. Un tel retard pourrait comporter un risque d'erreurs dans les états financiers et appeler à l'utilisation de contrôles adaptés afin de compenser ce risque.

L'objectif de l'auditeur, tel que prévu par la norme ISA 315, est d'identifier et d'évaluer le risque d'anomalies significatives provenant de fraudes ou d'erreurs dans les états financiers et assertions, par la connaissance de l'entité et de son environnement, y compris de son contrôle interne, lui permettant la conception et la mise en œuvre de réponses aux risques évalués d'anomalies significatives.

Dans la situation actuelle, une adaptation de son approche de contrôle en fonction du profil de risque modifié doit être envisagée.

## 6.3. Limitation d'un audit à distance

Afin de lutter contre cette pandémie, le télétravail a été imposé par le gouvernement belge pour toutes les fonctions qui le permettraient. Depuis le 4 mai 2020, il est fortement recommandé. Cette mesure implique le recours à des audits à distance. Ces derniers sont effectués grâce à des outils technologiques sécurisés et des moyens audiovisuels performants. Le contenu d'un audit à distance est identique à un audit physique. La seule différence réside dans le fait que les entretiens et la consultation de documents s'effectuent en ligne.

La possibilité de réaliser un audit de cette manière doit être évaluée en fonction de différents éléments :

- les caractéristiques de l'organisation contrôlée ;
- les infrastructures disponibles aussi bien chez l'auditeur que chez l'audité ;
- la phase de l'audit dans laquelle l'auditeur se trouve ;
- la composition de l'équipe d'audit.

Dans le cadre d'un audit à distance, les procédures indiquées dans la norme ISA 240, paragraphe 13, précisent : « À moins que l'auditeur n'ait de raison d'en douter, il peut accepter comme authentiques les enregistrements et les documents. Si des éléments identifiés au cours de l'audit le conduisent à penser qu'un document peut ne pas être authentique ou que les termes d'un document ont été modifiés sans que cela lui ait été mentionné, l'auditeur doit procéder à des investigations complémentaires. »

Bien qu'ils présentent des avantages au niveau de la documentation des procédures réalisées grâce aux échanges électroniques d'informations, les audits à distance peuvent conduire à certaines difficultés d'un point de vue pratique.

Tout d'abord, un audit à distance n'est pas toujours envisageable. En effet, une visite physique de l'organisation doit toujours être effectuée pour un lieu de production notamment.

De plus, l'auditeur est fortement dépendant des moyens technologiques auxquels il a recours. Il s'agit par exemple de la connexion internet ou de la stabilité des réseaux externes.

# Conclusion

Selon les normes ISA, la fraude consiste en « un acte intentionnel commis par une ou plusieurs personnes parmi les membres de la direction, les responsables de la gouvernance, les employés ou des tiers, impliquant le recours à des manœuvres trompeuses dans le but d'obtenir un avantage indu ou illégal. »

La fraude se scinde en deux catégories : la fraude externe et la fraude interne. La fraude externe comprend plusieurs types tels que l'espionnage industriel, la contrefaçon, la cybercriminalité, la fraude au président, les attaques informationnelles, la corruption. La fraude interne, l'objet de notre mémoire, concerne la fraude aux états financiers afin d'améliorer les résultats, et le détournement d'actifs dans le but d'un enrichissement personnel.

La fraude, peu importe la forme qu'elle revêt, obéit à un modèle élaboré par Donald R. Cressey, en vigueur depuis les années cinquante et expliquant les raisons d'un tel acte : le triangle de la fraude. Cette théorie repose sur trois piliers essentiels, à savoir la pression ressentie par le fraudeur, bien souvent de nature économique ou financière, l'opportunité de commettre une fraude qui peut se matérialiser notamment par une insuffisance de contrôles, et la rationalisation, c'est-à-dire la possibilité de justifier son acte. En 2004, ce modèle a été revu par Wolfe et Hermanson qui proposent d'ajouter une quatrième composante, à savoir la capacité de l'individu. Cette modélisation, nommée le diamant de la fraude, est particulièrement pertinente dans le cadre de l'évaluation du risque de fraude par l'auditeur.

Afin que la fraude ne soit pas une fatalité, il est impératif pour les organisations de disposer d'un environnement de contrôle interne performant. En vue de les assister dans cette tâche de grande ampleur, les entreprises disposent d'un allié de taille : le référentiel COSO Enterprise Risk Management (ERM). Ce référentiel est le plus largement répandu dans le cadre du contrôle interne et de la gestion des risques d'entreprise. Il reprend des lignes directrices relatives à des procédures de contrôle interne sur lesquelles la direction de l'entreprise peut se baser. Il est conçu en vue de soutenir des objectifs tels que : protéger les actifs, encourager les employés à respecter la politique de l'entreprise, garantir un enregistrement comptable précis et fiable en se conformant aux exigences légales.

Parallèlement à cet outil, il existe différentes mesures de prévention et de détection de la fraude interne : une structure de la gouvernance d'entreprise efficace pour les sociétés cotées,

l'élaboration d'un code de conduite précisant les comportements attendus et les pratiques interdites, un système de lancement d'alerte dont la nécessité est appuyée par une nouvelle directive européenne qui protège les individus signalant des cas de fraude et interdit toute forme de représailles à leur encontre, la mise en place de mesures d'accompagnement en cas de signaux d'alerte tel un changement de comportement d'un employé, le recours à des formations dont l'objectif est de sensibiliser le personnel à la problématique de fraude, la prise de sanctions appropriées en cas de fraude et la communication à l'ensemble du personnel et enfin, les outils d'analyse de données permettant de gérer le risque de fraude.

Pour détecter la fraude, les auditeurs utilisent des outils tels que l'analyse des ratios financiers, la méthode des séparateurs à vaste marge, les arbres de décision, le text mining, la loi de Benford.

Une des normes ISA est spécifiquement dédiée à la problématique de la fraude, l'ISA 240 « Responsabilités de l'auditeur concernant la fraude lors d'un audit d'états financiers ». Cette dernière rappelle que la direction d'une entité est responsable de l'élaboration et de la mise en œuvre d'un système de contrôle interne efficace. En revanche, la responsabilité de l'auditeur externe consiste à exprimer une opinion sur les états financiers pour lesquels il est tenu d'obtenir une assurance raisonnable que ceux-ci sont exempts d'inexactitudes importantes dues à la fraude ou à l'erreur. Pour ce faire, l'auditeur doit faire preuve de scepticisme professionnel en gardant à l'esprit la possibilité de contournement des contrôles en place par les dirigeants.

L'auditeur a une obligation de moyen et non de résultat, la fraude pouvant être de nature extrêmement sophistiquée et de facto difficile à identifier malgré un audit correctement planifié et exécuté. L'auditeur doit évaluer le risque de fraude et dispose également d'un rôle de prévention et de communication. Il est tenu de communiquer à la direction les faiblesses du contrôle interne relevées lors de l'audit ainsi que les cas de fraude identifiés ou soupçonnés. En cas de faiblesse des contrôles, les programmes d'audit devront être adaptés en ayant recours à davantage de tests de détail.

Il nous semblait essentiel de confronter toutes les informations recueillies de la littérature à la réalité du terrain. Nous nous sommes posé beaucoup de questions : « Que pensent les professionnels de ces outils théoriques et normatifs ? Ces derniers fonctionnent-ils efficacement ou sont-ils difficiles à implémenter ? ». Nous avons entrepris de mener une enquête en ligne auprès d'auditeurs externes et de réviseurs d'entreprises afin d'avoir leurs avis sur certaines

situations pouvant indiquer une fraude, sur l'efficacité de certaines mesures de prévention et sur l'utilisation des outils qu'ils utilisent. Les résultats obtenus ont été analysés et peaufinés grâce à des interviews que nous avons réalisées auprès de réviseurs d'entreprises attachés à de grands cabinets d'audit.

Cette étude nous a permis de dégager certaines tendances, de corroborer ou non certaines théories. Nous avons constaté que les cas de fraude sont souvent rencontrés, qu'il s'agit principalement de détournement d'actifs et qu'un environnement de travail ne tolérant aucun comportement frauduleux reste la mesure de prévention la plus efficace, mais doit être combinée avec d'autres mesures. Nous avons également relevé que les outils d'analyse de données les plus exploités par les professionnels de l'audit sont l'analyse des ratios financiers, les arbres de décision et la loi de Benford.

Cette partie du mémoire nous conforte dans notre décision d'avoir réalisé un travail conjoint. En effet, la recherche de contacts, l'administration d'un questionnaire auprès d'un nombre conséquent de répondants, l'analyse de tous les résultats, la rédaction d'un guide d'entretien détaillé et pertinent pour l'étude qualitative, les entretiens individuels à distance, leur retranscription et leur analyse nous ont demandé un travail non négligeable. En outre, la qualité de l'étude n'aurait pas atteint le même niveau si elle avait été menée de façon individuelle. En travaillant en binôme, l'analyse des résultats est plus pertinente, chacune apportant son point de vue, ses réflexions et ses critiques.

Nos études quantitative et qualitative se limitent aux réviseurs d'entreprises francophones. Si nous devions approfondir davantage le sujet, il serait intéressant d'étendre l'analyse auprès de réviseurs néerlandophones. L'enquête pourrait aussi être ouverte auprès d'entreprises belges, bien qu'elle soit probablement plus difficile à mener en raison de la confidentialité des informations.

La réalisation de ce mémoire nous a apporté un certain enrichissement personnel, notamment de par nos contacts avec des auditeurs et des réviseurs d'entreprises passionnés par leur travail. Nous nous rendons compte des exigences du métier et de l'expérience qu'il faut acquérir au fil des années pour mener à bien les missions qui sont confiées. Nous avons été motivées par ce sujet et notre curiosité a ouvert la porte d'une perspective professionnelle : les audits de fraude.

# Bibliographie


- Accouting.com. (2020). *What is forensic accounting ?* En ligne https://www.accounting.com/resources/forensic-accounting-basics/, consulté le 9 février 2020.
- Association of Certified Fraud Examiners. (2019). *Together, reducing fraud worldwide*. En ligne https://www.acfe.com/default.aspx, consulté le 20 août 2019.
- Bănărescu, A. (2015). Detecting and preventing fraud with data analytics. *Procedia Economics and Finance*, *vol.32*, 1827-1836. doi: 10.1016/S2212-5671(15)01485-9.
- Banque Nationale de Belgique. (2019). *Comptes annuels 2018 Pairi Daiza*. En ligne https://cri.nbb.be/bc9/web/catalog;jsessionid=578FD3CA7ACFBB3BFB133905077AA4DC?execution=e1s3, consulté le 17 avril 2020.
- BDO. (2019). *La fraude diminue, son coût augmente*. En ligne https://advisory.bdo.be/publications/la-fraude-diminue-son-cout-augmente/?lang=fr, consulté le 10 novembre 2019.
- BDO. (2020). *Prévenir la fraude*. En ligne https://www.bdo.be/fr-be/services/audit-assurance/forensics-litigation-services/prevention-de-fraude, consulté le 5 avril 2020.
- Bonache, A., Maurice, J., & Moris, K. (2010). Détection de fraudes et loi de Benford : quelques risques associés. *Revue Française De Comptabilité,* (431), 24-27. En ligne https://search-proquest-com.proxy.bib.ucl.ac.be:2443/docview/214146060?accountid=12156.
- Boyle, D.M., DeZoort, F.T., & Hermanson, D.R. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy*, *34*(6), 578-596. doi: 10.1016/j.jaccpubpol.2015.05.006.
- Charrier, E. (2004). Déceler les fraudes, les « Forensic Experts » en renfort des auditeurs. *Echanges*. En ligne https://core.ac.uk/download/pdf/6368957.pdf.

- Corporate governance committee. (2020). *Code belge de gouvernance d'entreprise 2020*. En ligne https://www.corporategovernancecommittee.be/fr/over-de-code-2020/code-belge-de-gouvernance-dentreprise-2020, consulté le 18 avril 2020.

- COSO. (2010). *Fraudulent financial reporting 1998-2007*. En ligne https://www.coso.org/Documents/COSO-Fraud-Study-2010-001.pdf, consulté le 6 avril 2020.

- Creswell, J.W. (2013). *Research design: Qualitative, quantitative, and mixed method approaches.* (4è éd.). SAGE Publications.

- Dalnial, H., Kamaluddin, A., Sanusi, Z.M., & Khairuddin, K.S. (2014). Accountability in financial reporting: detecting fraudulent firms. *Procedia - Social and Behavioral Sciences, vol.145,* 61-69. doi: 10.1016/j.sbspro.2014.06.011.

- Deloitte. (2017). *Deloitte bribery and corruption survey 2017*. En ligne https://www2.deloitte.com/nz/en/pages/risk/articles/2017-bribery-and-corruption-survey.html, consulté le 12 novembre 2019.

- DH.be. (2019). *Cybercriminalité : l'Europe lutte contre les logiciels pirates*. En ligne https://www.dhnet.be/actu/new-tech/cybercriminalite-l-europe-lutte-contre-les-logiciels-pirates-5c9b83b87b50a60b4559a03a, consulté le 27 août 2019.

- Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union. (2019). *Journal officiel de l'Union européenne L305, 26 novembre 2019.*

- Ernst & Young. (2018). *Comment gérer le risque de non-compliance à l'ère de la transformation digitale?* En ligne https://www.ey.com/Publication/vwLUAssets/ey-global-forensic-data-analytics-survey-2018-fr/$FILE/ey-global-forensic-data-analytics-survey-2018.pdf, consulté le 30 janvier 2020.

- Ernst & Young. (2018). *Integrity in the spotlight: The future of compliance (15th global fraud survey).* En ligne https://www.ey.com/Publication/vwLUAssets/EY_Global_Fraud_Survey_2018_report/$FILE/EY%20GLOBAL%20FIDS%20FRAUD%20SURVEY%202018.pdf, consulté le 12 novembre 2019.

- Ernst & Young. (2014). *Overcoming compliance fatigue: Reinforcing the commitment to ethical growth (13th global fraud survey)*. En ligne https://www.ey.com/Publication/vwLUAssets/EY-13th-Global-Fraud-Survey/$FILE/EY-13th-Global-Fraud-Survey.pdf, consulté le 12 novembre 2019.

- Gomez, C. (2017). Contrefaçon et terrorisme : comprendre les mécanismes. *Revue internationale et stratégique*, 2017/3 (n°107), 32-40. En ligne https://www-cairn-info.proxy.bib.ucl.ac.be:2443/revue-internationale-et-strategique-2017-3-page-32.htm#.

- Guetterman, T., & Creswell, J.W. (2018). Educational research: Planning, conducting, and evaluating quantitative and qualitative research (6è éd.). Pearson.

- Harrell, M.C., & Bradley, M.A. (2009). *Data collection methods: Semi-structured interviews and focus groups.* RAND Corporation. En ligne https://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR718.pdf.

- Hassid, O., Masraff, A. (2010). *La sécurité en entreprise : prévenir et gérer les risques*. Paris : Maxima.

- ICCI. (2020). FAQ COVID-19 : impact sur le contrôle interne et le risque de fraude et audit à distance. En ligne https://www.icci.be/fr/actualit/actualit-detail-page/faq-covid-19-impact-sur-le-contr-le-interne-et-le-risque-de-fraude-et-audit-distance?fbclid=IwAR2TOF9B3YFUxvmP6gGwI2f5-WK8iY5iz4ZqIephluLkb6E-DeORn1jE3AE, consulté le 6 avril 2020.

- International Accounting Standards Board. (2016). *IFRS 15, Revenue from contracts with customers.*

- IRE. (2017). *Communication 2017/15 : Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces*. En ligne https://www.ibr-ire.be/fr/reglementation-et-publications/doctrine/communications/communication-2017-15, consulté le 11 février 2020.

- IRE. (2019). *La profession*. En ligne https://2019.rapportannuelire.be, consulté le 11 mai 2020.

- ISO. (s.d.). *ISO/IEC 27001 Management de la sécurité de l'information*. En ligne https://www.iso.org/fr/isoiec-27001-information-security.html, consulté le 16 août 2019.

- Kanapickienė, R., & Grundienė, Ž. (2015). The model of fraud detection in financial statements by means of financial ratios. *Procedia - Social and Behavioral Sciences, vol.213,* 321-327. doi: 10.1016/j.sbspro.2015.11.545.

- KPMG. (2016). *Global profiles of the fraudster: Technology enables and weak controls fuels the fraude.* En ligne https://assets.kpmg/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf, consulté le 13 novembre 2019.

- Le Maux, J., Smaili, N., & Ben Amar, W. (2013). De la fraude en gestion à la gestion de fraude. *Revue française de gestion, 39*(231), 73-85. doi:10.3166/rfg.231.73-85.

- Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice, 16*(4), 473–475. doi:10.1177/1524839915580941.

- Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à l'utilisation des espèces (2017). *Moniteur belge, 6 février, p.90839.*

- Mohamed, N., & Handley-Schachler, M. (2015). Roots of responsibilities to financial statement fraud control. *Procedia Economics and Finance, vol.28,* 46-52. doi: 10.1016/S2212-5671(15)01080-1.

- Mohd-Sanusi, Z., Khalid, N.H., & Mahir, A. (2015). An evaluation of clients' fraud reasoning motives in assessing fraud risks: from the perspective of external and internal auditors. *Procedia Economics and Finance, vol.31,* 2-12. doi: 10.1016/S2212-5671(15)01126-0.

- International Federation of Accountants. (2017). *ISA 240, Les obligations de l'auditeur en matière de fraude lors d'un audit d'états financiers*.

- International Federation of Accountants. (2017). *ISA 315 (Révisée), Identification et évaluation des risques d'anomalies significatives par la connaissance de l'entité et de son environnement.*

- PakAccountants.com. (2016). *ISA 240 – The auditor's responsibilities relating to fraud in an audit of financial statements*. En ligne https://pakaccountants.com/standards/isa/isa240/, consulté le 8 février 2020.

- Perrin, B., De Preux, P. (2018). *L'investigation en entreprise : prévention et détection des fraudes*. Presses polytechniques et universitaires romandes.

- Petraşcu, D., & Tieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance, vol.16,* 489-497. doi: 10.1016/S2212-5671(14)00829-6.

- Protiviti. (2014). *The updated COSO internal control framework*. En ligne https://www.protiviti.com/sites/default/files/united_states/insights/updated-coso-internal-control-framework-faqs-third-edition-protiviti.pdf, consulté le 11 décembre 2019.

- PwC. (2016). *Assessing the risk of bribery and corruption to your business*. En ligne https://www.pwc.com.au/pdf/assessing-the-risk-of-bribery-and-corruption-oct2016.pdf, consulté le 12 novembre 2018.

- PwC. (2020). *Fighting fraud: A never-ending battle. PwC's Global economic crime and fraud survey*. En ligne https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf, consulté le 9 mai 2020.

- Razali, W.A.A.W.M., & Arshad, R. (2014). Disclosure of corporate governance structure and the likelihood of fraudulent financial reporting. *Procedia - Social and Behavioral Sciences, vol.145,* 243-253. doi: 10.1016/j.sbspro.2014.06.032.

- Romney, M. B. & Steinbart, P. J. (2016). *Accounting Information Systems* (14è éd.). New York: Pearson.

- RTBF info. (2017). *La « fraude au CEO », ou comment les escrocs arrivent à se faire passer pour le président*. En ligne https://www.rtbf.be/info/economie/detail_la-fraude-au-ceo-ou-comment-les-escrocs-arrivent-a-se-faire-passer-pour-le-president?id=9674926, consulté le 13 novembre 2019.

- RTBF info. (2019). *La Louvière : une comptable suspectée d'avoir détourné 30.000€ du port autonome*. En ligne https://www.rtbf.be/info/regions/detail_la-louviere-une-comptable-suspectee-d-avoir-detourne-30-000-du-port-autonome?id=10295012, consulté le 22 août 2019.

- Sadgali, I., Sael, N., & Benabbou, F. (2019). Performance of machine learning techniques in the detection of financial frauds. *Procedia Computer Science*, *vol.148*, 45-54. doi : 10.1016/j.procs.2019.01.007.

- Saunders, M., & Tosey, P. (2013). The layers of research design. En ligne https://www.academia.edu/4107831/The_Layers_of_Research_Design.

- Taskin, L. (2017-2018). *Management humain*. Document non publié, Université Catholique de Louvain, Mons.

- The Institute of Internal Auditors. (2017). *Normes internationales pour la pratique professionnelle de l'audit interne*. En ligne https://na.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-French.pdf, consulté le 17 janvier 2020.

- Transparency International. (s.d.). *What is corruption ?* En ligne https://www.transparency.org/what-is-corruption#define, consulté le 13 novembre 2019.

- Vessié, B. (2018-2019). Contrôle interne et gestion des risques. Document non publié, Université Catholique de Louvain, Mons.

- Vitez, O. (2019). *What is management override of internal controls ?* En ligne https://bizfluent.com/facts-6052778-management-override-internal-controls-.html, consulté le 12 novembre 2019.

- West, J., Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. *Computers & Security*, *vol.57*, 47-66. doi: 10.1016/j.cose.2015.09.005.

- Wolfe, D., & Hermanson, D.R. (2004). The fraud diamond: considering the four elements of fraud. *CPA Journal*, 38-42. En ligne https://pdfs.semanticscholar.org/c9c8/32fa299f648464cbd0172ff293f5c35684b6.pdf.

- Zager, L., Sever Malis, S., & Novak, A. (2016). The role and responsibility of auditors in prevention and detection of fraudulent financial reporting. *Procedia Economics and Finance, vol.39,* 693-700. doi: 10.1016/S2212-5671(16)30291-X.

**UNIVERSITÉ CATHOLIQUE DE LOUVAIN**
**Louvain School of Management**
Chaussée de Binche 151, 7000 Mons, Belgique | **www.uclouvain.be/lsm**